SECTORAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORISM FINANCING

IN CYBERCRIME

2024

SECTORAL RISK ASSESSMENT OF MONEY LAUNDERING AND TERRORISM FINANCING IN CYBERCRIME 2024

Book Size	:	295 x 210 mm
Manuscript	:	Sectoral Risk Assessment of Money Laundering and Terrorism Financing in Cybercrime 2024
Published by	:	Financial Transaction Reports and Analysis Center

FURTHER INFORMATION

Indonesian Financial Transaction Reports and Analysis Center (INTRAC)

Jl. Ir. H. Juanda No. 35 Jakarta 10120 Indonesia

Phone: (+6221) 3850455, 3853922

Fax: (+6221) 3856809 – 3856826

Website: http://www.ppatk.go.id

TEAM

A. Steering Committee

1. Chief of the Criminal Chamber, Supreme Court of the Republic of Indonesia
2. Head of the AML/CFT Group, Financial Services Authority (OJK)
3. Deputy Attorney General for Special Crimes, Attorney General's Office of the Republic of Indonesia
4. Director of Transnational and Terrorism Crimes, Attorney General's Office of the Republic of Indonesia
5. Director of Special Economic Crimes, Criminal Investigation Agency (Bareskrim) of the Indonesian National Police (POLRI)
6. Director of Cybercrime, Bareskrim POLRI
7. Director of Investigation, Densus 88 Anti-Terror Police Unit
8. Director of Intelligence, Densus 88 Anti-Terror Police Unit
9. Director of Cyber and National Encryption Security, National Cyber and Encryption Agency (BSSN)
10. Director of Informatics Application Control, Ministry of Communication and Informatics (c.q. Director of Application Control, Ministry of Communication and Informatics)
11. Director of Domestic Strategy and Cooperation, INTRACT
12. Director of International Strategy and Cooperation, INTRACT
13. Director of Reporting, INTRACT
14. Director of Compliance Supervision for Financial Service Providers, INTRACT
15. Director of Analysis and Examination I, INTRACT
16. Director of Analysis and Examination II, INTRACT
17. Director of Analysis and Examination III, INTRACT
18. Director of Law and Regulation, INTRACT
19. Head of Partnership Empowerment Center for AML–CFT, INTRACT
20. Head of the Payment System Policy Department, Bank Indonesia
21. Head of the Bureau of Commodity Futures Trading Supervision, Warehouse Receipt System, and Commodity Auction Market, Commodity Futures Trading Supervisory Agency
22. Head of the Bureau of Legislation and Law Enforcement, Commodity Futures Trading Supervisory Agency

B. Implementation Team

1. Representative of the Supreme Court
    1) R. Heru Wibowo Sukaten
    2) Dwi Sugiarto
2. Representative of the Deputy Attorney General for Special Crimes, Attorney General's Office of the Republic of Indonesia
    1) Suyanto Reksasumarta
    2) Bagus Gede Mas Widipradnyana Arjaya
3. Representative of the Directorate of Transnational and Terrorism Crimes, Attorney General's Office of the Republic of Indonesia
    1) Erwin Indraputra

2) Herry Wijayatno

4. Representative of the Directorate of Cybercrime, Criminal Investigation Agency of the Indonesian National Police
   1) I Made Redi Hartana
   2) Eko Yudha Prasetya
5. Representative of the Directorate of Special Economic Crimes, Criminal Investigation Agency of the Indonesian National Police
   1) Ertata Hamonangan Sinaga
   2) Dwi Martono
6. Representative of the Special Anti-Terror Detachment, Indonesian National Police
   1) Daniel
   2) Jay Kesuma
   3) Sadewa Fradana Santoso
7. Representative of the Directorate of Cyber and National Encryption Security, National Cyber and Encryption Agency
   1) Dony Harso
   2) Fredy Ramadani
8. Representative of the Directorate of Informatics Application Control, Ministry of Communication and Informatics (c.q. Director of Application Control, Ministry of Communication and Informatics)
   1) Jelitha Suina Putri
   2) Ryan Abdisa Sukmadja
9. Representative of the Financial Services Authority
   1) Rifki Arif Budianto
   2) Marshella Eka Ramdhania
10. Representative of Bank Indonesia
    1) Danarto Tri Sasongko
    2) Nabila Femiliana
11. Representative of the Commodity Futures Trading Supervisory Agency, Ministry of Trade
    1) Hary Lesmana
    2) Yovian Andri Prihandono
    3) Rio Ramadhani
12. Internal INTRACT
    1) Diana Soraya Noor
    2) Patrick Irawan
    3) Tri Puji Raharjo
    4) Mardiansyah
    5) Vidyata A. A.
    6) Sheilla Yudiana
    7) Kristina Widhi P.
    8) Riana Rizka
    9) Dini Rahayu
    10) Aditya Akbar Apriyadi
    11) Jesse Octavillisia
    12) Ade Novita Rosseani
    13) Ibrahim Arifin
    14) Muhammad Afdal Yanuar
    15) Nelmy Pulungan
    16) Rusli Safrudin
    17) Dominicus Suseno
    18) Puri Widyaksari
    19) Damai Tri Putri
    20) Andi Emil Arya Hidayat
    21) Nur Sofia Arianti
    22) Didin Najmudin

EXECUTIVE SUMMARY

Cybercrime is one of the predicate offenses (TPA) of Money Laundering (ML). Cybercrime incidents tend to increase year after year, both in Indonesia and globally. Indonesia's digital economy growth, which is among the highest in Southeast Asia, underscores the increasing importance of addressing cybercrime.

To mitigate ML and TF (Terrorism Financing) risks arising from cybercrime in Indonesia, a sectoral risk assessment was prepared to identify cybercrime risk factors so that risk mitigation can be carried out effectively and efficiently. With technological developments, crimes may be committed using cyberspace, but for the scope of this study, cybercrime is limited to offenses under the Electronic Information and Transactions Law (Law No. 11 of 2016 and its amendments).

The Cybercrime ML/TF Sectoral Risk Assessment (SRA) aims to identify, analyze, evaluate, and mitigate ML and TF risks arising from cybercrime by identifying the types of cybercrimes with ML/TF potential in Indonesia; and identifying and analyzing ML/TF risks based on cybercrime type, offender profile, reporting sector, region, typologies, and transaction patterns. The guidelines used in preparing the 2024 Cybercrime SRA refer to international best practices from the National Money Laundering and Terrorist Financing Assessment (FATF Guidance), Risk Assessment Support for Money Laundering/Terrorist Financing (World Bank), Review of the Fund's Strategy on Anti-Money Laundering and Terrorist Financing (IMF), and Terrorist Financing Risk Assessment Guidance.

Using data from January 2019 to March 2024, sourced from statistics on suspicious transaction reports, supervisory activities, FIU (financial intelligence unit) information exchange, financial intelligence reports, investigation, prosecution, and court rulings, as well as self-assessments by experts or representatives of reporting parties, supervisory and regulatory bodies, FIUs (INTRACT), and law enforcement agencies, the ML and TF risks arising from cybercrime were assessed. Qualitative data collection was carried out through questionnaires submitted to supervisory and regulatory authorities, law enforcement agencies, relevant ministries/institutions, and reporting parties—36 respondents with an average response rate of 94%. In addition to questionnaires, interviews were conducted with 4 supervisory/regulatory representatives, four (4) law enforcement representatives, and two (2)

ministry/institution representatives from reporting parties to obtain deeper insight into ML and TF risks related to cybercrime.

The key findings of the 2024 Cybercrime ML/TF SRA are as follows:

1. No evidence has been found of a shift in cybercrime/ITE risk as a predicate offense for ML since the 2021 NRA. ML risk from cybercrime remains relatively low, supported by the small number of cybercrime cases linked to or proven as ML.
2. By cybercrime type, online fraud is assessed as high-risk for ML.
3. By profile, entrepreneurs/self-employed persons and private-sector employees are considered high-risk profiles for ML from cybercrime. Indonesian nationals (WNI) are also assessed as high-risk. Proceeds of cybercrime tend to be laundered by the offenders themselves.
4. By region, Jakarta is assessed as high-risk for ML arising from cybercrime.
5. By the industrial sector of the reporting party, banks are assessed as high-risk.
6. By ML typology, the highest-risk activities are the use of virtual assets and online gambling.
7. By transaction pattern, the highest-risk activities are transfers and cash withdrawals/deposits.
8. Singapore, the United States, Hong Kong, the People's Republic of China, India, and Malaysia are considered by respondents as countries that may serve as sources, destinations, or transit points for ML proceeds from cybercrime.
9. TF risk could not be measured in this study due to limited case data. However, given the existence of cyber fraud cases used to fund TF abroad, this potential must be monitored.
10. Misuse of financial technology (e.g., crypto assets) and cyberspace for communication, propaganda, and recruitment has occurred and must be closely monitored by law enforcement.

Furthermore, several developments identified by stakeholders as having the potential to be widely exploited in the future—based on observations of suspicious financial transactions and developments in ML/TF case handling—include:

1. Misuse of AI
2. Misuse of e-wallets
3. Use of coin-mixing services
4. Dissemination of links/files containing viruses or attempts to take over user data
5. Use of private wallet addresses
6. Exploitation of Web3 and crypto assets

FOREWORD

The rapid development of technology helps society meet various needs, but it also brings potential risks of crime such as theft, fraud, misuse, and other forms of criminal activity. In 2023, the FATF released the report Illicit Financial Flows from Cyber-Enabled Fraud. The report highlights cyber-enabled fraud as an emerging form of transnational organized crime. In Indonesia, based on data from Pusiknas POLRI (National Criminal Information Center of Indonesian National Police) in 2022, cybercrime increased significantly—by fourteen times—compared with the same period in 2021.

Cybercrime causes significant financial losses and has negative impacts on government, infrastructure, and industry—not only in Indonesia but also globally. The effects of cybercrime can also be felt at the individual level, such as identity theft, account breaches, and email compromise schemes. Preventing and combating cybercrime is not only the responsibility of law enforcement agencies, but also of various stakeholders. One of the measures taken by INTRACT is the preparation of a sectoral risk assessment to understand the Money Laundering and Terrorism Financing risks arising from cybercrime in Indonesia.

Therefore, I welcome the preparation of the 2024 Sectoral Risk Assessment of Money Laundering and Terrorism Financing in Cybercrime, and I hope it will be followed by strategic actions and mitigation efforts addressing the evolving risks that have been identified by all relevant stakeholders. Finally, I extend my gratitude and appreciation to all parties who contributed to the preparation of the 2024 Sectoral Risk Assessment of Money Laundering and Terrorism Financing in Cybercrime.

Jakarta, December 2024

[signed]

Dr. Ivan Yustiavandana, S.H., LL.M.

Head of the Financial Transaction Reports and Analysis Center

LIST OF ABBREVIATIONS AND TERMS

No.	Abbreviation/Term	Definition
1	AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
2	ASEAN	Association of Southeast Asian Nations
3	BSSN	National Cyber and Encryption Agency
4	Dark Web	World Wide Web content on the *darknet* requiring special software, configuration, or authorization.
5	FATF	Financial Action Task Force on Money Laundering
6	Foreign Predicate Crime	ML committed abroad and laundered in Indonesia
7	IMF	International Monetary Fund
8	Interpol	International Criminal Police Organization
9	NRA	National Risk Assessment
10	POLRI	Indonesian National Police
11	Ransomware	Malicious software that threatens victims by destroying or blocking access until ransom is paid
12	Robinopsnal Bareskrim POLRI	Operational Development Bureau, Criminal Investigation Agency, Indonesian National Police
13	SRA	Sectoral Risk Assessment
14	TP	Criminal Act
15	TPA	Predicate Offense
16	TPPT	Terrorism Financing
17	TPPU	Money Laundering
18	UU ITE	Electronic Information and Transactions Law
19	WNA	Foreign Citizen
20	WNI	Indonesian Citizen

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER I

INTRODUCTION

1.1 Background

The term cyber in the The Great Dictionary of the Indonesian Language (KBBI) refers to computer and information systems, cyberspace, or matters related to the internet. Cybercrime is a criminal act involving the internet, computer systems, or computer technology. In the explanatory section of Law of the Republic of Indonesia Number 19 of 2016 on Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (the ITE Law), it is stated that[1]:

"*... the characteristic of cyberspace virtuality enables illegal content such as Electronic Information and/or Electronic Documents containing materials that violate decency, gambling, insults or defamation, extortion and/or threats, dissemination of false and misleading news resulting in consumer losses in Electronic Transactions, acts of spreading hatred or hostility based on ethnicity, religion, race, and societal groups, and the transmission of threats of violence or intimidation directed at individuals to be accessed, distributed, transmitted, copied, stored for further dissemination from anywhere and at any time*."

This statement has become increasingly relevant amid rapidly advancing technology. Technological development helps society meet various needs, but it also brings potential risks of crime, such as theft, fraud, misuse, and other criminal activities.

In Indonesia, based on data from the National Police Cyber Unit (Pusiknas POLRI), cybercrime increased significantly in 2022—by fourteen times—compared with the same period in 2021. In 2023, the FATF released the report *Illicit Financial Flows from Cyber-*

[1] The latest provisions concerning the ITE Law are contained in Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions."

Enabled Fraud, which stated that cyber-enabled fraud is an emerging form of transnational organized crime. According to the *2023 Interpol Global Crime Trend Summary Report*, there has been a significant increase in the sophistication and volume of cyberattacks and cyber-enabled crime, including child sexual exploitation and financial fraud. The use of crime-as-a-service[2] has had a notable impact on the expansion of such crimes.

CYBERCRIME INCREASED MORE THAN TENFOLD

Period 1 Jan to 22 December 2021 Number of enforcement actions: 612 cases Number of units taking action: 26 out of 35 units	**Period 1 Jan to 22 December 2022** Number of enforcement actions: 8,831 cases Number of units taking action: 35 or all units
7 Units with the Highest Number of Enforcement Actions Polda Metro Jaya 293 cases East Java Regional Police 60 cases South Sulawesi Regional Police 58 cases West Java Regional Police 48 cases North Sumatra Regional Police 40 cases Criminal Investigation Agency (Bareskrim Polri) 21 cases Lampung Regional Police 18 cases	**7 Units with the Highest Number of Enforcement Actions** Polda Metro Jaya 3,709 cases South Sulawesi Regional Police 962 cases North Sumatra Regional Police 896 cases East Java Regional Police 648 cases West Java Regional Police 409 cases Lampung Regional Police 295 cases North Sulawesi Regional Police 167 cases
The number of enforcement actions against cybercrime in Indonesia increased fourteenfold in 2022 compared with 2021. The number of working units carrying out enforcement also increased. Data source: *e-MP Robinopsnal Bareskrim Polri, accessed on Friday, 23 December 2022 at 10:30 WIB*	

Figure 1 Cybercrime Increased More Than Tenfold

[2] Crime-as-a-Service refers to services that enable the commission of crimes. Examples of Crime-as-a-Service include hacking services, the sale of personal data used to gain access to financial data, and money-laundering services.

Source:: https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali kali_lipat

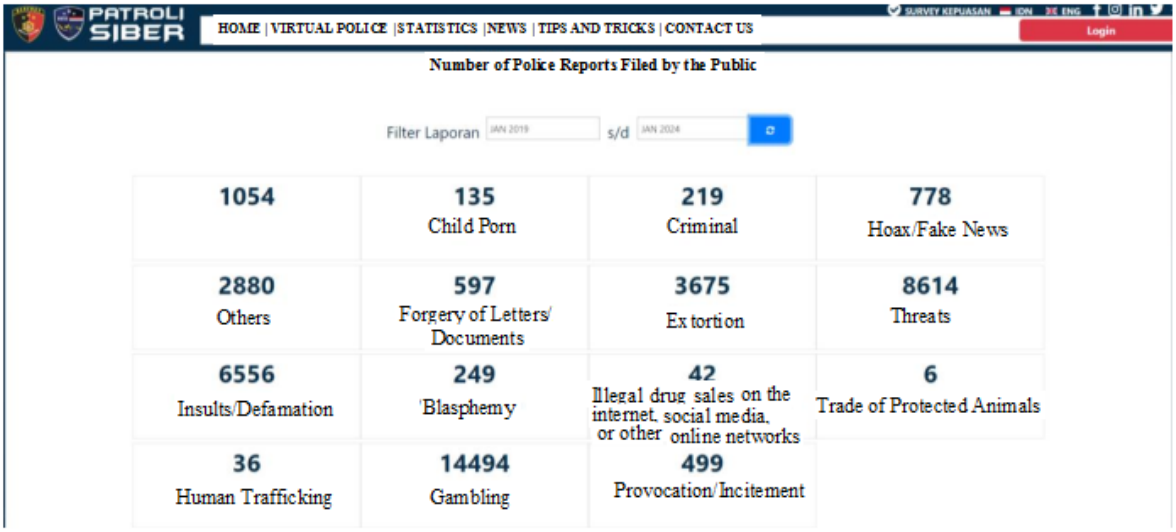

Figure 2 Statistics on the Number of Police Reports Filed by the Public Related to Cybercrime

Source: Patrolisiber.id

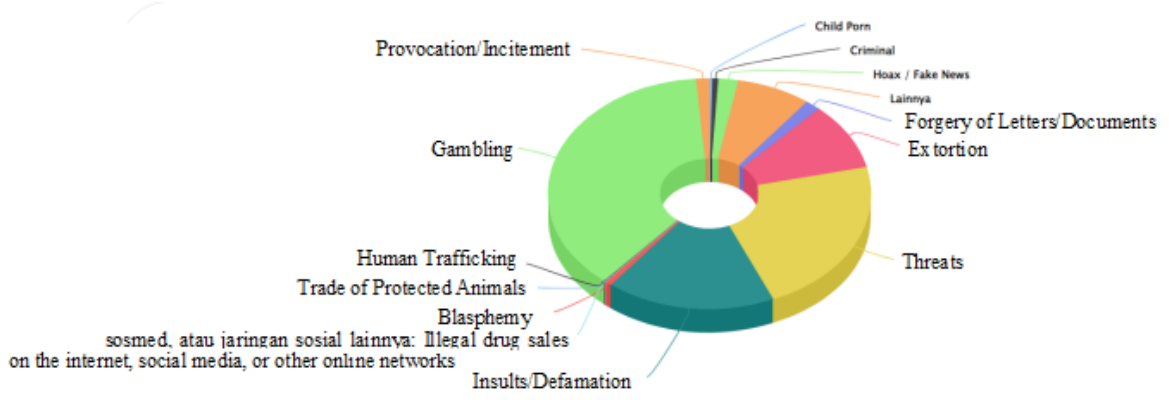

Figure 3 Pie Chart of Police Reports Filed by the Public Related to Cybercrime

Source: Patrolisiber.id

The growth of the digital economy has also made the handling of cybercrime increasingly important. In 2022, Indonesia's digital economy recorded the highest value in Southeast Asia, reaching USD 77 billion, equivalent to 40% of ASEAN's internet economy

market share. Cybersecurity is also one of the main pillars of efforts to develop Indonesia's digital economy, which is expected to strengthen public trust and encourage participation in the digital economy. According to the Interpol Cyber Assessment Report (2021), during the period of January–September 2020, a total of 2.7 million ransomware attacks were detected in ASEAN countries. Indonesia ranked first, with 1.3 million cases. In addition, data breaches caused by cybercrime are projected to result in global economic losses of up to USD 5 trillion by 2024. Efforts to enhance cybersecurity are not only a concern for law enforcement agencies, but also for regulators such as the Ministry of Communication and Informatics and the National Cyber and Encryption Agency.

Cybercrime is one of the predicate offenses for money laundering (ML) in Indonesia, as cyber offenses fall under other criminal acts punishable by four (4) years of imprisonment or more. In the 2021 National Risk Assessment (NRA), it was found that fraud, corruption, fund transfer, narcotics, and electronic information and transactions (ITE) or cyber-related offenses are predicate crimes categorized as high-risk for ML under foreign predicate crime (ML that occurs abroad while the laundering takes place in Indonesia), although cybercrime in general is assessed as low-risk for ML. In 2022, INTRACT prepared the Sectoral Risk Assessment on Money Laundering in Cyber Fraud. The development of cybercrime in Indonesia has been so rapid that the Indonesian National Police (Polri) plans to establish a special directorate for cybercrime handling in nine regions across the country.

To mitigate ML and TF risks arising from cybercrime in Indonesia, one of the efforts that can be undertaken is preparing a sectoral risk assessment to identify cybercrime risk factors so that risk mitigation can be carried out effectively and efficiently. Therefore, a Sectoral Risk Assessment (SRA) on ML and TF risks from cybercrime needs to be conducted.

1.2 Objectives

The SRA study on ML and TF arising from Cybercrime is intended to identify, analyze, evaluate, and mitigate ML and TF risks originating from Cybercrime, with the specific objectives to:

1. Identify the types of cybercrime that have the potential to generate ML and TF in Indonesia;
2. Identify and analyze ML and TF risks arising from cybercrime in Indonesia;
3. Identify and analyze ML and TF risks arising from cybercrime in Indonesia based on ML and TF typologies;
4. Identify and analyze ML and TF risks arising from cybercrime in Indonesia based on the reporting-sector industries exploited in ML and TF;
5. Identify and analyze ML and TF risks arising from cybercrime in Indonesia based on transaction patterns used by offenders;
6. Identify and analyze ML and TF risks arising from cybercrime in Indonesia based on regions or provinces; and
7. Identify and analyze ML and TF risks arising from cybercrime in Indonesia based on offenders' occupational profiles and nationality profiles.

1.3 Output

The expected outputs of this study include:

1. Strengthening and updating the understanding of ML and TF risks arising from cybercrime;
2. Supporting ministries/institutions and the private sector in aligning national and institutional controls and mitigation strategies through improved understanding of ML and TF risks originating from cybercrime; and
3. Enabling reporting parties to pay greater attention to and enhance the detection of suspicious transaction reports related to cybercrime.

CHAPTER II

LITERATURE REVIEW

2.1 History of Cybercrime

Cybercrime is defined as "criminal activities in which a computer or computer network becomes the tool, target, or place where the crime occurs" (Aziz, 2019). Cybercrime can be divided into two major categories: Computer Crime, namely attempts to infiltrate or gain unauthorized electronic access to systems, services, resources, or electronic information; and Computer-Enabled Crime, namely illegal activities (such as fraud, money laundering, identity theft) that are conducted or facilitated by electronic systems and devices, such as networks and computers.

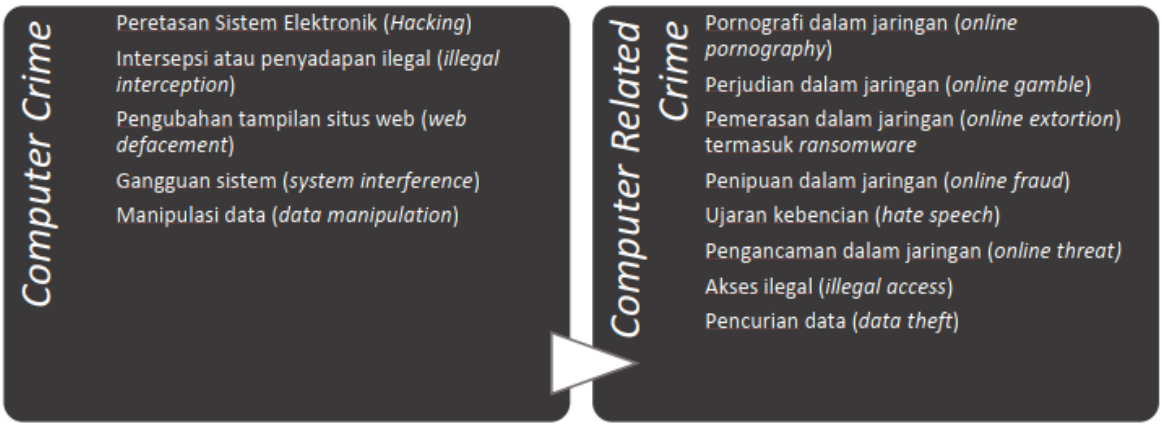

Figure 4 Computer Crime and Computer-Enabled Crime

Source: Patrolisiber.id

The first recorded "cyber" offense occurred in France in 1834 (Wolf, 2024). At that time, the offender infiltrated the French telegraph system and stole financial market data. The first modern cybercrime is believed to have been committed by Allen Scherr in 1962, when he stole passwords from a punch-card database and subsequently carried out an attack on the Massachusetts Institute of Technology (MIT) computer network. In 1971, the world's first computer virus was created by Bob Thomas, although the virus was never released into a computer system. In 1981, Ian Murphy became the first person arrested for a cybercrime after hacking into AT&T's systems and causing chaos by altering the time settings in the company's

computer systems. Then, in 1988, Robert Morris released the Morris Worm, regarded as one of the first major cyberattacks on the internet. The first ransomware appeared in 1989.

During the 1990s, Vladimir Levin became known as the first hacker to attempt a bank robbery. In 1995, he hacked into Citibank's systems and transferred more than USD 10 million into several bank accounts around the world. Although the first computer virus was created in 1971, computer viruses remained relatively unknown to the public until the emergence of the Melissa virus in March 1999. The virus was hidden in an online document that promised access to adult content; once opened, it took over the user's Microsoft Word application, moved into Microsoft Outlook, and spread by emailing itself to multiple accounts. This virus caused losses of around USD 80 million and was one of the first major viruses to spread beyond AOL (America Online, a multinational mass media company).

The first cybercrime prosecuted in Indonesia occurred in 1988 (Dimila, 2019). At that time, the BNI 1946 New York branch account was hacked by Rudy Demsy, a former BNI New York employee. Since then, numerous cybercrime cases have taken place in Indonesia, targeting not only government websites but also online stores or e-commerce platforms and other websites with cybersecurity vulnerabilities. One global case that also affected Indonesia was the WannaCry ransomware attack, which infected more than 200,000 computers in 2017 (Anjelina & Afifah, 2024). As mentioned in the background section, cybercrime in Indonesia increased fourteenfold between 2021 and 2022. To mitigate the growing threat of cybercrime, Cybercrime Investigation Directorates in eight Regional Police Offices (North Sumatra, Metro Jaya, West Java, Central Java, East Java, Bali, Central Sulawesi, and Papua) were officially established on 20 September 2024 (R., 2024).

2.2 Cybercrime Convention

The Cybercrime Convention (Convention on Cybercrime), or the Budapest Convention, is the first international treaty that seeks to address internet and computer crime (cybercrime) by harmonizing national laws, improving investigative techniques, and enhancing cooperation among countries. The convention was adopted on 8 November 2001, and as of April 2023, 68 countries worldwide have ratified it, while two countries (Ireland and South Africa) have signed but not ratified it. Indonesia has not ratified the Budapest Convention, but several aspects of Indonesia's cybercrime regulations are derived from the Convention. The criminal offenses regulated in the Budapest Convention include:

A. Offences against the confidentiality, integrity, and availability of computer data and systems illegal access
    a. Illegal interception
    b. Data interference
    c. System interference
    d. Misuse of devices
B. Computer-related offences
    a. Computer-related forgery
    b. Computer-related fraud
C. Content-related offences
    a. Offences related to child pornography
D. Offences related to infringements of copyright and related rights
E. Ancillary liability and sanctions
    a. Attempt and aiding or abetting
    b. Corporate liability

2.3 Cybercrime Regulation in Indonesia

Cybercrime in Indonesia is regulated under Law Number 11 of 2008 on Electronic Information and Transactions, Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions, and Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions. The key provisions on cybercrime in Indonesia are as follows:

Table 1 Cybercrime Regulations in Indonesia

No.	Offense	Criminal Sanctions	Parallelism with the Budapest Convention
1.	Article 27 paragraph (1) of Law No. 1 of 2024 Any Person who intentionally and without right broadcasts, displays, distributes, transmits, and/or makes accessible Electronic Information and/or Electronic Documents containing content that violates decency for public knowledge.	Article 45 paragraph (1) of Law No. 1 of 2024 (1) Any Person who intentionally and without right broadcasts, displays, distributes, transmits, and/or makes accessible Electronic Information and/or Electronic Documents containing content that violates decency for public knowledge as referred to in Article 27 paragraph (1) shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). Article 52 of Law Number 11 of 2008 (1) In the event that the criminal act as referred to in Article 27 paragraph (1) concerns decency or sexual exploitation of a child, the punishment shall be increased by one-third of the principal penalty. Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	Content-Related Offense
2.	Article 27 paragraph (2) of Law No. 1 of 2024 Any Person who intentionally and without right distributes, transmits, and/or makes accessible Electronic Information	Article 45 paragraph (3) of Law No. 1 of 2024 (3) Any Person who intentionally and without right distributes, transmits, and/or makes accessible Electronic Information and/or Electronic Documents containing gambling content	Content-Related Offense

	and/or Electronic Documents containing gambling content.	as referred to in Article 27 paragraph (2) shall be punished with imprisonment of up to 10 (ten) years and/or a fine of up to Rp10,000,000,000.00 (ten billion rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
3.	Article 27A of Law No. 1 of 2024 Any Person who intentionally attacks the honor or good name of another person by attributing something to that person, with the intention that such accusation becomes publicly known, in the form of Electronic Information and/or Electronic Documents, carried out through an Electronic System.	Article 45 paragraph (4) of Law No. 1 of 2024 (4) Any Person who intentionally attacks the honor or good name of another person by attributing something to that person, with the intention that such accusation becomes publicly known, in the form of Electronic Information and/or Electronic Documents carried out through an Electronic System as referred to in Article 27A, shall be punished with imprisonment of up to 2 (two) years and/or a fine of up to Rp400,000,000.00 (four hundred million rupiah). (6) In the event that the act referred to in paragraph (4) cannot be proven true and contradicts what is actually known while the offender has been given the opportunity to prove it, the offender shall be punished for defamation with imprisonment of up to 4 (four) years and/or a fine of up to Rp750,000,000.00 (seven hundred fifty million rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the	Content-Related Offense

		principal penalty shall be increased by two-thirds.	
4.	Article 27B of Law No. 1 of 2024 (1) Any Person who intentionally and without authority distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent of unlawfully benefiting himself/herself or another person, compels a person, by threats of violence, to: a. surrender an item, whether in whole or in part, belonging to that person or to another person; or b. grant a loan, make an acknowledgment of debt, or discharge a receivable.	Article 45 paragraph (8) of Law No. 1 of 2024 (8) Any person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit himself/herself or another person, by forcing a person through threats of violence to: a. hand over an item, in whole or in part, belonging to that person or to another person; or b. grant a loan, make an acknowledgment of debt, or extinguish a receivable, as referred to in Article 27B paragraph (1), shall be punished by imprisonment for a maximum of six (6) years and/or a fine of up to IDR 1,000,000,000 (one billion rupiah). Article 52 paragraph (4) of Law No. 11 of 2008 In the event that a criminal offence referred to in Articles 27 to 37 is committed by a corporation, the principal penalty shall be increased by two-thirds.	Content-Related Offense
4.	Article 27B of Law No. 1 of 2024 (2) Any Person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or another person, by means of threats of defamation or	Article 45 paragraph (10) of Law No. 1 of 2024 (10) Any Person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents, with the intent to unlawfully benefit themselves or another person, by means of threats of defamation or threats to reveal a secret, thereby coercing another person to: a. give an item, whether partially or wholly belonging to that person or to	Content-Related Offense

	threats to reveal a secret, thereby coercing another person to: a. give an item, whether partially or wholly belonging to that person or to another person; or b. provide a loan, make an acknowledgment of debt, or discharge a receivable.	another person; or b. provide a loan, make an acknowledgment of debt, or discharge a receivable, as referred to in Article 27B paragraph (2), shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
5.	Article 28 of Law No. 1 of 2024 (1) Any Person who intentionally and/or without right transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that result in material losses to consumers in an Electronic Transaction.	Article 45A of Law No. 1 of 2024 (1) Any Person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false notifications or misleading information that result in material losses to consumers in an Electronic Transaction as referred to in Article 28 paragraph (1), shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	Computer-related fraud
6.	Article 28 of Law No. 1 of 2024	Article 45A paragraph (2) of Law No. 1 of 2024	Content-Related Offense

	(2) Any Person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents that incite, invite, or influence others in a manner that generates feelings of hatred or hostility toward certain individuals and/or groups of people based on race, nationality, ethnicity, skin color, religion, belief, gender, mental disability, or physical disability.	(2) Any Person who intentionally and without right distributes and/or transmits Electronic Information and/or Electronic Documents that incite, invite, or influence others in a manner that generates feelings of hatred or hostility toward certain individuals and/or groups of people based on race, nationality, ethnicity, skin color, religion, belief, gender, mental disability, or physical disability as referred to in Article 28 paragraph (2), shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
7.	Article 28 of Law No. 1 of 2024 (3) Any Person who intentionally spreads Electronic Information and/or Electronic Documents that they know contain false notifications which cause public unrest.	Article 45A paragraph (3) of Law No. 1 of 2024 (3) Any Person who intentionally spreads Electronic Information and/or Electronic Documents that they know contain false notifications which cause public unrest as referred to in Article 28 paragraph (3), shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp1,000,000,000.00 (one billion rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by	Content-Related Offense

		two-thirds.	
8.	Article 29 of Law No. 1 of 2024 Any Person who intentionally and without right sends Electronic Information and/or Electronic Documents directly to a victim containing threats of violence and/or intimidation.	Article 45B of Law No. 1 of 2024 Any Person who intentionally and without right sends Electronic Information and/or Electronic Documents directly to a victim containing threats of violence and/or intimidation as referred to in Article 29, shall be punished with imprisonment of up to 4 (four) years and/or a fine of up to Rp750,000,000.00 (seven hundred fifty million rupiah). Article 52 paragraph (4) of Law Number 11 of 2008 (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	Content-Related Offense
9.	Article 30 of Law Number 11 of 2008 (1) Any Person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System belonging to another Person in any manner. (2) Any Person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System in any manner with the purpose of obtaining Electronic Information and/or Electronic Documents. (3) Any Person who intentionally and without right or unlawfully accesses	Article 46 of Law Number 11 of 2008 (1) Any Person who fulfills the elements as referred to in Article 30 paragraph (1) shall be punished with imprisonment of up to 6 (six) years and/or a fine of up to Rp600,000,000.00 (six hundred million rupiah). (2) Any Person who fulfills the elements as referred to in Article 30 paragraph (2) shall be punished with imprisonment of up to 7 (seven) years and/or a fine of up to Rp700,000,000.00 (seven hundred million rupiah). (3) Any Person who fulfills the elements as referred to in Article 30 paragraph (3) shall be punished with imprisonment of up to 8 (eight) years and/or a fine of up to Rp800,000,000.00 (eight hundred million rupiah). Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008	Illegal Access

	a Computer and/or Electronic System in any manner by violating, circumventing, exceeding, or breaching the security system.	(2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions—including but not limited to defense agencies, the central bank, banking institutions, financial institutions, international organizations, or aviation authorities—the maximum principal penalty under each Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
10.	Article 31 of Law Number 19 of 2016 (1) Any Person who intentionally and without right or unlawfully conducts interception or wiretapping of Electronic Information and/or Electronic Documents within a particular Computer and/or Electronic System belonging to another Person. (2) Any Person who intentionally and without right or unlawfully conducts	Article 47 of Law Number 11 of 2008 Any Person who fulfills the elements as referred to in Article 31 paragraph (1) or paragraph (2) shall be punished with imprisonment of up to 10 (ten) years and/or a fine of up to Rp800,000,000.00 (eight hundred million rupiah). Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public	Illegal Interception

	interception of the transmission of Electronic Information and/or Electronic Documents that are non-public in nature, from, to, or within a particular Computer and/or Electronic System belonging to another Person—whether the interception does not cause any change or causes changes, deletion, and/or termination of the Electronic Information and/or Electronic Documents being transmitted.	services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions—including but not limited to defense agencies, the central bank, banking institutions, financial institutions, international organizations, or aviation authorities—the maximum principal penalty under each Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
11.	Article 32 of Law Number 11 of 2008 (1) Any Person who intentionally and without right or unlawfully, in any manner, alters, adds to, subtracts from, transmits, damages, deletes, transfers, moves, or conceals Electronic Information and/or Electronic Documents belonging to another Person or owned by the public. (2) Any Person who intentionally and without right or unlawfully, in any manner, transfers or transmits Electronic Information and/or Electronic Documents to	Article 48 of Law Number 11 of 2008 (1) Any Person who fulfills the elements as referred to in Article 32 paragraph (1) shall be punished with imprisonment of up to 8 (eight) years and/or a fine of up to Rp2,000,000,000.00 (two billion rupiah). (2) Any Person who fulfills the elements as referred to in Article 32 paragraph (2) shall be punished with imprisonment of up to 9 (nine) years and/or a fine of up to Rp3,000,000,000.00 (three billion rupiah). (3) Any Person who fulfills the elements as referred to in Article 32 paragraph (3) shall be punished with imprisonment of up to 10 (ten) years and/or a fine of up to Rp5,000,000,000.00 (five billion rupiah). Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008	Data Interference

	another Person's Electronic System that is not entitled to receive such information or documents. (3) In relation to the act as referred to in paragraph (1), where such act results in Electronic Information and/or Electronic Documents of a confidential nature becoming accessible to the public with data integrity that is not properly maintained.	(2) In the event that the acts referred to in Articles 30 through 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 through 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions—including but not limited to defense agencies, the central bank, banking institutions, financial institutions, international organizations, or aviation authorities—the maximum principal penalty under each Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
12.	Article 33 of Law Number 11 of 2008 Any Person who intentionally and without right or unlawfully commits any act that results in the disruption of an Electronic System and/or causes an Electronic System to fail to function properly.	Article 49 of Law Number 11 of 2008 Any Person who fulfills the elements as referred to in Article 33 shall be punished with imprisonment of up to 10 (ten) years and/or a fine of up to Rp10,000,000,000.00 (ten billion rupiah). Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public	

		services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions—including but not limited to defense agencies, the central bank, banking institutions, financial institutions, international organizations, or aviation authorities—the maximum principal penalty under each Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	
13.	Article 34 of Law Number 11 of 2008 (1) Any Person who intentionally and without right or unlawfully produces, sells, makes available for use, imports, distributes, provides, or possesses: a. computer hardware or software designed or specifically developed to facilitate acts as referred to in Articles 27 to 33; b. computer passwords, access codes, or similar means intended to enable access to an Electronic System for the purpose of facilitating acts as referred to in Articles 27 to 33.	Article 50 of Law Number 11 of 2008 Any Person who fulfills the elements as referred to in Article 34 paragraph (1) shall be punished with imprisonment of up to 10 (ten) years and/or a fine of up to Rp10,000,000,000.00 (ten billion rupiah). Article 52 paragraphs (2) and (3) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or	Misuse of Devices

		Electronic Documents owned by the Government and/or strategic institutions—including but not limited to defense institutions, the central bank, banking institutions, financial institutions, international organizations, or aviation authorities—the maximum principal penalty under each Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the principal penalty shall be increased by two-thirds. Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 through 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions, including but not limited to defense institutions, the central bank, banking, financial institutions, international organizations, and aviation authorities, the maximum principal penalty under each relevant Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 through 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	

14.	Article 35 of Law Number 11 of 2008 Any Person who intentionally and without right or unlawfully performs manipulation, creation, alteration, deletion, or destruction of Electronic Information and/or Electronic Documents with the purpose of causing such Electronic Information and/or Electronic Documents to be considered as if they were authentic data.	Article 51 of Law Number 11 of 2008 (1) Any Person who fulfills the elements as referred to in Article 35 shall be punished with imprisonment of up to 12 (twelve) years and/or a fine of up to Rp12,000,000,000.00 (twelve billion rupiah). (2) Any Person who fulfills the elements as referred to in Article 36 shall be punished with imprisonment of up to 12 (twelve) years and/or a fine of up to Rp12,000,000,000.00 (twelve billion rupiah).	Computer-related forgery and fraud
15.	Article 36 of Law Number 11 of 2008 Any Person who intentionally and without right commits acts as referred to in Articles 30 through 34 that result in material losses to another Person.	Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions, including but not limited to defense institutions, the central bank, banking institutions, financial institutions, international organizations, and aviation authorities, the maximum principal penalty under each relevant Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 to 37 are	

		committed by a corporation, the principal penalty shall be increased by two-thirds.	
16.	Article 37 of Law Number 11 of 2008 Any Person who intentionally commits acts prohibited as referred to in Articles 27 to 36 outside the territory of Indonesia against an Electronic System located within the jurisdiction of Indonesia.	Article 52 paragraphs (2), (3), and (4) of Law Number 11 of 2008 (2) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or used for public services, the principal penalty shall be increased by one-third. (3) In the event that the acts referred to in Articles 30 to 37 are directed at Computers and/or Electronic Systems as well as Electronic Information and/or Electronic Documents owned by the Government and/or strategic institutions, including but not limited to defense institutions, the central bank, banking institutions, financial institutions, international organizations, and aviation authorities, the maximum principal penalty under each relevant Article shall be increased by two-thirds. (4) In the event that the criminal acts referred to in Articles 27 to 37 are committed by a corporation, the principal penalty shall be increased by two-thirds.	

CHAPTER III

RESEARCH METHODOLOGY

3.1 RESEARCH METHOD

The research methodology used in the 2024 Cyber Sectoral Risk Assessment (Cyber SRA) is a mixed-method explanatory sequential design. This methodology is a combination that integrates qualitative and quantitative research methods sequentially. The quantitative approach uses statistical data derived from suspicious transaction reports, supervisory activities, information exchange between financial intelligence units (FIU), financial intelligence reports, investigations, prosecutions, and court rulings. Meanwhile, the qualitative approach uses self-assessments conducted by experts or specialists from reporting parties, supervisory and regulatory authorities, the financial intelligence unit (INTRACT), and law enforcement agencies regarding the quality of prevention and eradication measures for money laundering and terrorism financing crimes related to cybercrime.

The guidelines used in the preparation of the 2024 Cyber SRA refer to international best practices from the National Money Laundering and Terrorist Financing Assessment (FATF Guidance), Risk Assessment Support for Money Laundering/Terrorist Financing (World Bank), Review of the Fund's Strategy on Anti-Money Laundering and Terrorist Financing (IMF), and Terrorist Financing Risk Assessment Guidance.

3.2 SCOPE AND STEPS OF RISK ASSESSMENT

The scope of the 2024 Cyber SRA includes identifying types of cybercrime that have the potential to generate money laundering (ML) and terrorism financing (TF) risks in Indonesia, as well as identifying and analyzing ML and TF risks arising from cybercrime in Indonesia. These risks are assessed based on ML and TF typologies, the reporting party's

industrial sectors exploited in ML and TF activities, regions or provinces, and offender profiles.

The FATF Guidance explains that risk is formulated as a function as follows:

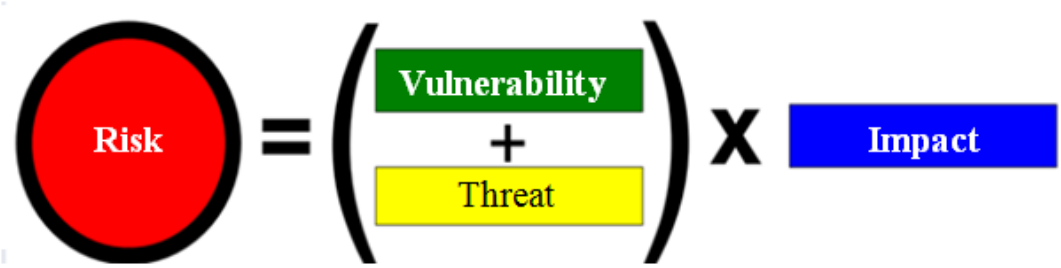

Figure 5 Risk Assessment Formulation

a. Threat, refers to a person or group of persons, an object, or an activity that has the potential to cause harm, for example to a country, society, the economy, and others. In the ML/TF context, this includes criminals, terrorist groups and their facilitators, their funds, as well as past, present, and future money laundering or terrorism financing activities.
b. Vulnerability, refers to factors that can be exploited by a threat or that can support or facilitate its activities. In the context of ML/TF risk assessment, viewing vulnerabilities as distinct from threats means focusing, for example, on factors representing weaknesses in the AML/CFT system or controls, or specific characteristics of a country. This may also include features of certain sectors, financial products, or types of services that make them attractive for ML or TF purposes.
c. Likelihood, refers to the probability of the occurrence of money laundering and terrorism financing activities.
d. Consequence, refers to the effects or losses that may result from ML or TF and includes the impact of the underlying criminal and terrorist activities on financial systems and institutions, as well as on the economy and society in general. The consequences of ML or TF may be short-term or long-term and may also relate to specific populations or communities, the business environment, or national or international interests, as well as the reputation and attractiveness of a country's financial sector.
e. Emerging Trend, refers to new and/or evolving channels used as means for money laundering and terrorism financing before their impacts become widely evident.

3.3 STAGES OF RISK ASSESSMENT

In preparing the 2024 Cyber Sectoral Risk Assessment (Cyber SRA), several stages of activities were carried out throughout 2024, as follows:

A. Preparation Stage

1. Preparation of the 2024 Cyber SRA proposal in January 2024.
2. Internal presentation of the 2024 Cyber SRA proposal in February 2024.
3. Formation of the internal and external teams for the preparation of the 2024 Cyber SRA in March 2024.
4. Meetings with regulators, law enforcement agencies, and Ministries/Agencies regarding the urgency of preparing the Cyber SRA in April 2024.

B. Implementation Stage

a. Risk Identification

This stage involved identifying the risk factors to be analyzed, as well as identifying the types of data and information required.

b. Risk Analysis

The risk analysis stage was conducted as a continuation of the risk identification stage, using the variables of vulnerability, threat, and consequence. The purpose of this stage was to analyze the identified risk factors in order to understand their nature, sources, likelihood, and consequences, and to assign relative risk levels to each risk factor.

c. Risk Evaluation

This stage involved the process of synthesizing the findings from the risk analysis phase to determine priorities for addressing risks, taking into account the objectives of the risk assessment established at the beginning of the process. This stage also contributed to the development of risk mitigation strategies aimed at addressing the identified risks.

C. Launch or Dissemination Stage

launch or dissemination stage was carried out to provide shared understanding and to raise awareness regarding sectoral ML and TF risks related to cybercrime in 2024. The implementation of the launch or dissemination included the following activities:

1. Finalization of the report in December 2024.
2. Launch and communication of the results of the 2024 Cyber SRA Report to regulators, law enforcement agencies, and relevant Ministries/Agencies, scheduled to be conducted in 2025.

3.4 DATA SOURCES

The preparation of the 2024 Cyber Sectoral Risk Assessment (Cyber SRA) was conducted using data from the period January 2019 to March 2024. The quantitative approach employed statistical data sourced from suspicious financial transaction reports, supervisory activities, information exchange between financial intelligence units (FIU), financial intelligence reports, investigations, prosecutions, and court decisions. Meanwhile, the qualitative approach utilized self-assessments conducted by experts from representatives of reporting parties, supervisory and regulatory authorities, the FIUs (INTRACT), and law enforcement agencies. All of this data and information were used to identify, analyze, and evaluate the risks of money laundering and terrorism financing arising from cybercrime.

Qualitative data collection was carried out through the distribution of questionnaires to supervisory and regulatory authorities, law enforcement agencies, relevant ministries/agencies, and reporting entities, involving a total of 36 respondents, with an average response rate of 94%, detailed as follows:

a. 4 respondents from 4 supervisory and regulatory authorities with an average response rate of 100%;
b. 5 respondents from 5 law enforcement agencies with an average response rate of 100%;
c. 1 respondent from 1 relevant ministry/agency with an average response rate of 100%; and
d. 24 respondents from 26 reporting entities with an average response rate of 92%.

In addition to questionnaires, data collection was also conducted through interviews with four representatives of supervisory and regulatory authorities, four representatives of law enforcement agencies, and two relevant ministries/agencies, to obtain deeper insights into the risks of money laundering and terrorism financing related to cybercrime. The topics discussed in the SRA questionnaires and interviews included, among others:

Table 2 SRA Questionnaire and Interview Topics

Questionnaire	Interview
1. Perceptions of threats, vulnerabilities, and impacts of ML and TF arising from each type of cybercrime per PoC. 2. Number of cases and monetary values (investigations, prosecutions, and court decisions) related to ML and TF involving financial technology (fintech) by type of cybercrime (for law enforcement agencies only). 3. Case studies. 4. Risk mitigation measures for ML and TF related to cybercrime.	1. Perceptions of the likelihood of ML and TF arising from cybercrime (conventional or digital). 2. Institutional policies for the prevention and eradication of cybercrime and/or ML and TF. 3. New or emerging ML and TF threats arising from cybercrime. 4. Indicators of suspicious ML and TF transactions related to cybercrime. 5. Capabilities of reporting entities in detecting suspicious financial transactions and in fulfilling case data requirements, supervision of reporting entities, and the handling of cybercrime and/or ML and TF cases. 6. Forms of domestic and international cooperation. 7. Challenges. 8. Recommendations: a. Prevention sector b. Enforcement sector c. Cooperation sector

CHAPTER IV

RISK ASSESSMENT RESULTS

4.1 Risk Assessment Results

A. ML Risk Level

Based on court decisions successfully collected, only a small number of money laundering (ML) cases originated from cybercrime (8 cases) when compared to the total number of ML court decisions during the study period (January 2019 to March 2024). According to the Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) Statistical Bulletin, the total number of ML court decisions from January 2020 to June 2024 amounted to 673 cases. The National Risk Assessment on Money Laundering Crime (2021) stated that the risk of ITE-related crimes serving as predicate offenses for ML is Low, and the analysis of court decision data in this study has not found evidence of any shift from this Low risk level. While cybercrime is prevalent, relatively few cases are charged with ML or proven to involve ML.

Based on questionnaire results, respondents assessed the likelihood that cybercrime offenders are also ML offenders as moderate/reasonably possible. In cases identified in Indonesia, it was found that some cybercrime offenders were also ML offenders. In addition to assessing whether cybercrime offenders are also ML offenders, interviews explored whether cybercrime offenders tend to conduct money laundering through instrumental digital laundering (only one stage of money laundering conducted digitally) or integral digital laundering (all stages of money laundering conducted digitally). The results showed that the majority of respondents (67%) believed that cybercrime offenders tend to engage in integral digital laundering. In identified cases, offenders not only conducted money laundering digitally but, in some instances, still used savings accounts (traditional methods).

The ML risk assessment arising from cybercrime based on the previously determined PoCs can be summarized as follows:

1. ML Risk Level Based on the Type of Cybercrime

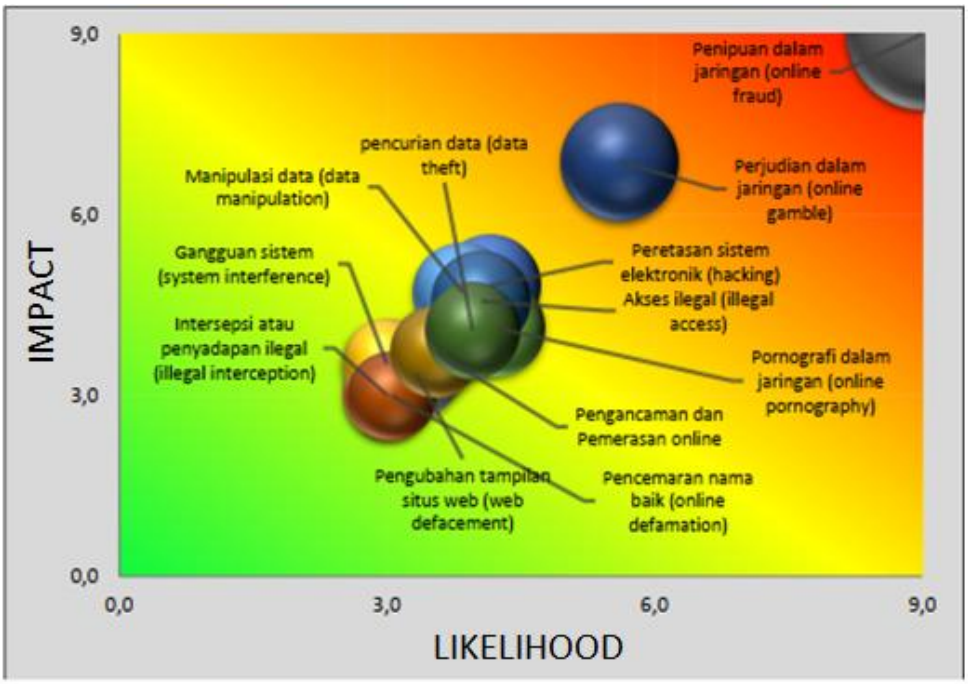

Figure 6 ML Risk Level from Cybercrime Based on Cybercrime Type

Online fraud is assessed as a type of cybercrime with a high ML (money laundering) risk. Based on data from e-MP Robinopsnal Bareskrim POLRI as of 23 December 2022, fraud committed through electronic media ranked as the second most common cybercrime handled by the Indonesian National Police (2,131 cases), after manipulation of authentic data (3,723 cases) for the period 1 January to December 2022 (Pusiknas Bareskrim POLRI, n.d.). In 2023, fraud cases ranked first, with a total of 1,414 cases (Tribratanews.polri.go.id, 2023). Meanwhile, online gambling is assessed as having a medium ML risk. Other types of cybercrime are assessed as having a low ML risk.

2. ML Risk Level Based on the Offender Profile

Entrepreneurs/self-employed individuals and private-sector employees are assessed as profiles with a high ML risk arising from cybercrime. Students, traders, professionals and consultants, legislative and government officials, and bank employees are assessed as posing a medium ML risk arising from cybercrime. Legislative and government officials are considered to have a medium risk due to the identification of several online gambling cases involving government officials. Other profiles are considered to pose a low ML risk.

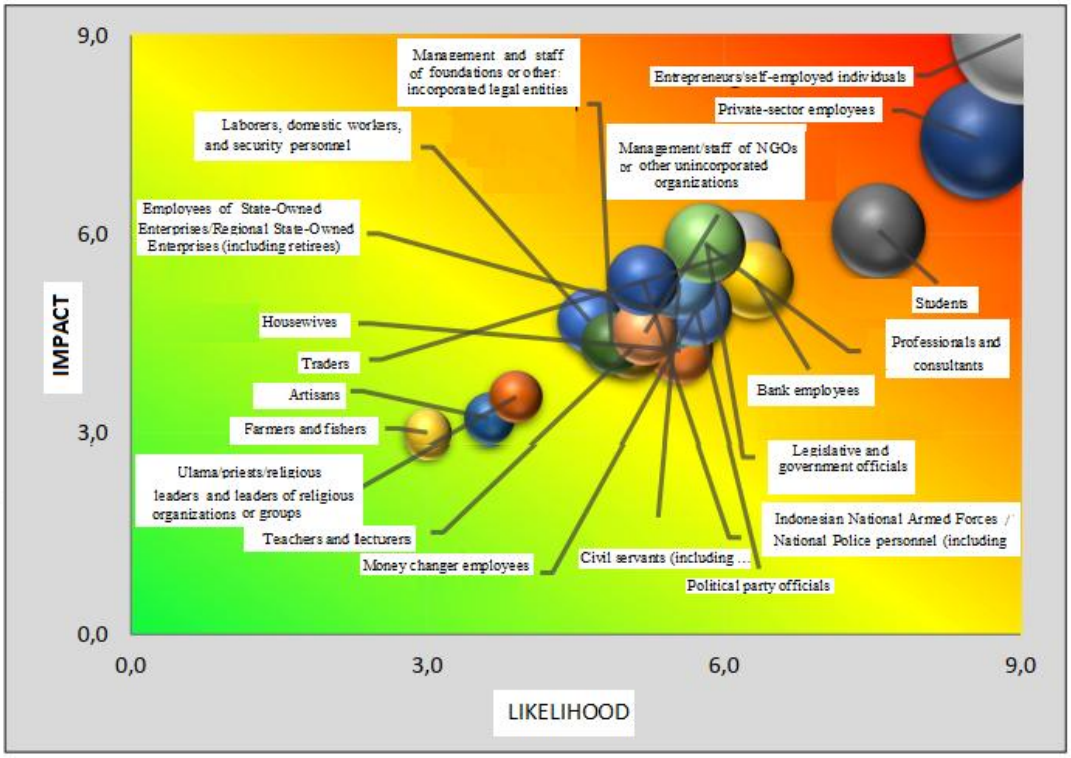

Figure 7 ML Risk Level from Cybercrime Based on Offender Profile

3. ML Risk Level from Cybercrime Based on Region

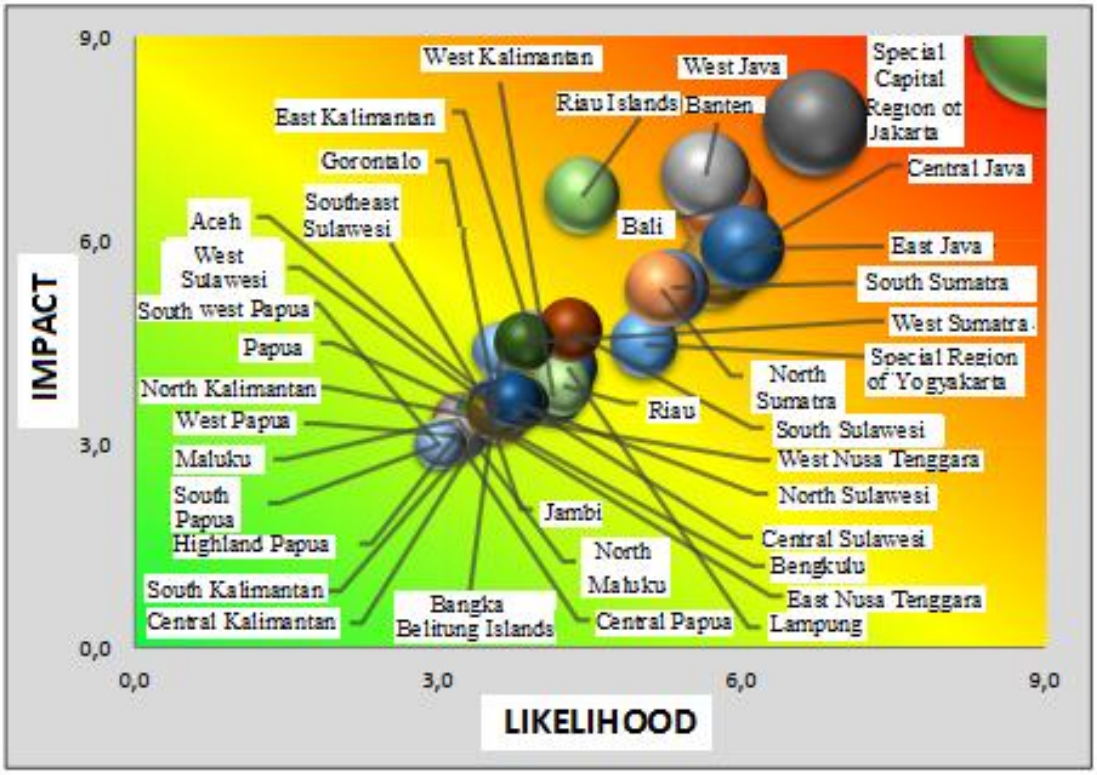

Figure 8 Risk Level of ML from Cybercrime Based on Region

Cybercrime essentially occurs in cyberspace, which is not confined to any specific geographic boundaries. However, for the purposes of this study, data were obtained on the locations of incidents or courts handling cybercrime cases. DKI Jakarta is assessed as having a high ML risk based on regional classification, while West Java, Banten, Bali, and East Java are assessed as posing a medium ML risk.

4. ML Risk Level from Cybercrime Based on the Nationality of Cybercrime Offenders

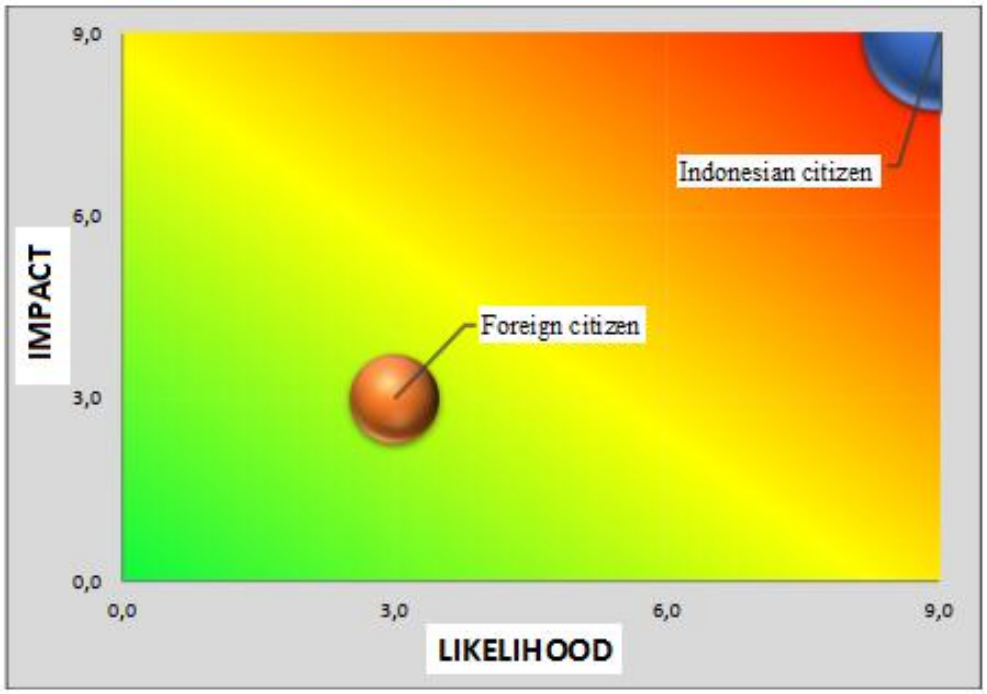

Figure 9 ML Risk Level Based on Nationality of Cybercrime Offenders

Indonesian nationals (WNI) are assessed as posing a high ML risk arising from cybercrime, while foreign nationals (WNA) are assessed as having a low ML risk. In several cybercrime cases, foreign nationals have indeed been involved; for example, a case involving 103 foreign nationals who misused residence permits and were suspected of engaging in cybercrime (Special Class I Immigration Office TPI Batam, 2024). Despite the existence of the principle of territoriality under the Indonesian Criminal Code (KUHP), it is not always possible to impose criminal sanctions on foreign nationals in Indonesia. Moreover, in the context of cybercrime, foreign offenders may be located abroad, making it difficult to prosecute them in Indonesia.

5. ML Risk Level from Cybercrime Based on the Role of Cybercrime Offenders

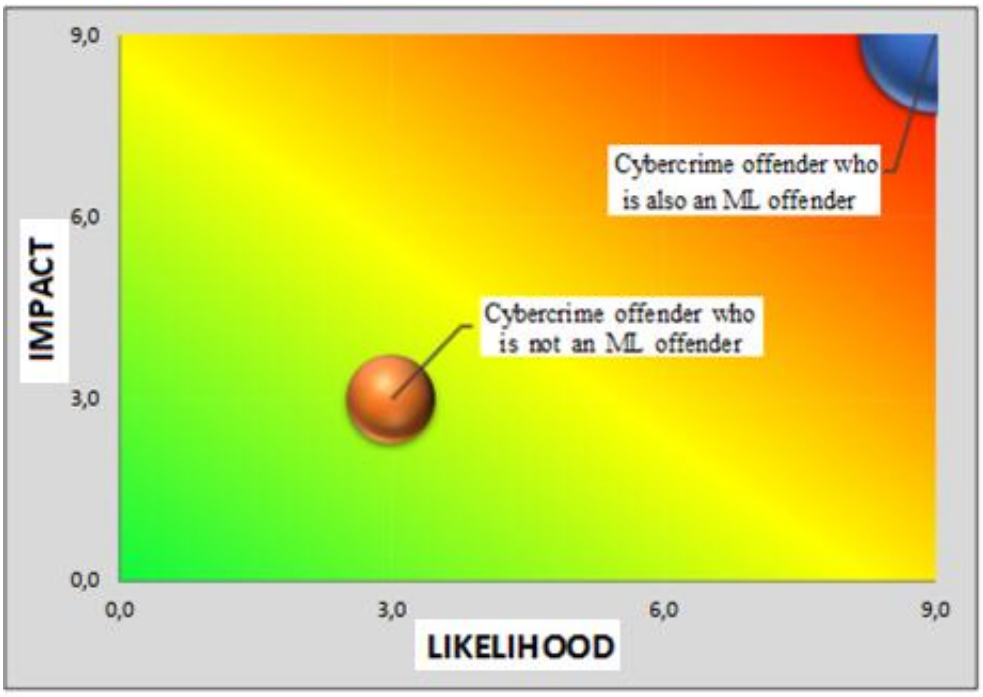

Figure 10 ML Risk Level from Cybercrime Based on the Role of Cybercrime Offenders

Based on the assessment results, it was found that in ML cases arising from cybercrime identified in Indonesia, cybercrime offenders tend also to be ML offenders.

6. ML Risk Level from Cybercrime Based on the Reporting-Entity Industry Sector

The banking sector is assessed as posing a high ML risk arising from cybercrime. Meanwhile, physical crypto asset traders are assessed as posing a medium ML risk, and other reporting entities are assessed as posing a low ML risk. ML offenders deriving proceeds from cybercrime continue to extensively misuse the banking sector for money laundering, although there is an emerging shift toward the use of crypto assets.

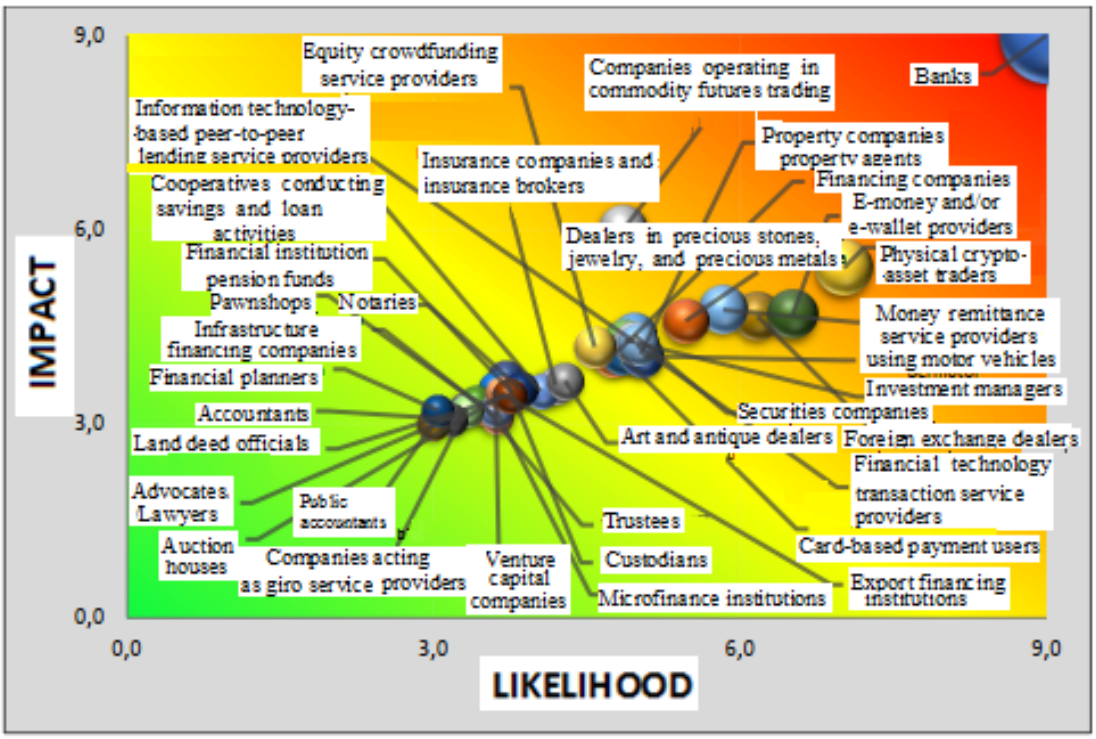

Figure 11 Risk Level of ML from Cybercrime Based on Reporting Sector Industryqqqqaaq

7. Money Laundering Risk Level of Cybercrime Proceeds Based on ML Typologies

The money laundering (ML) typologies arising from cybercrime that are assessed as high risk in Indonesia are the use of virtual currencies and online gambling. The use of virtual currencies/crypto-assets in this context is not necessarily facilitated by domestic Physical Crypto-Asset Traders, as crypto-assets can be obtained not only through domestic Physical Crypto-Asset Traders, but also through mining, peer-to-peer transactions, and Physical Crypto-Asset Traders operating abroad. When crypto-asset transactions are conducted through Physical Crypto-Asset Traders in Indonesia, it is easier for law enforcement agencies to trace them, as Physical Crypto-Asset Traders constitute one of the reporting parties. However, when offenders use the services of foreign Physical Crypto-Asset Traders, Indonesian law enforcement agencies face significant challenges in tracing such transactions.

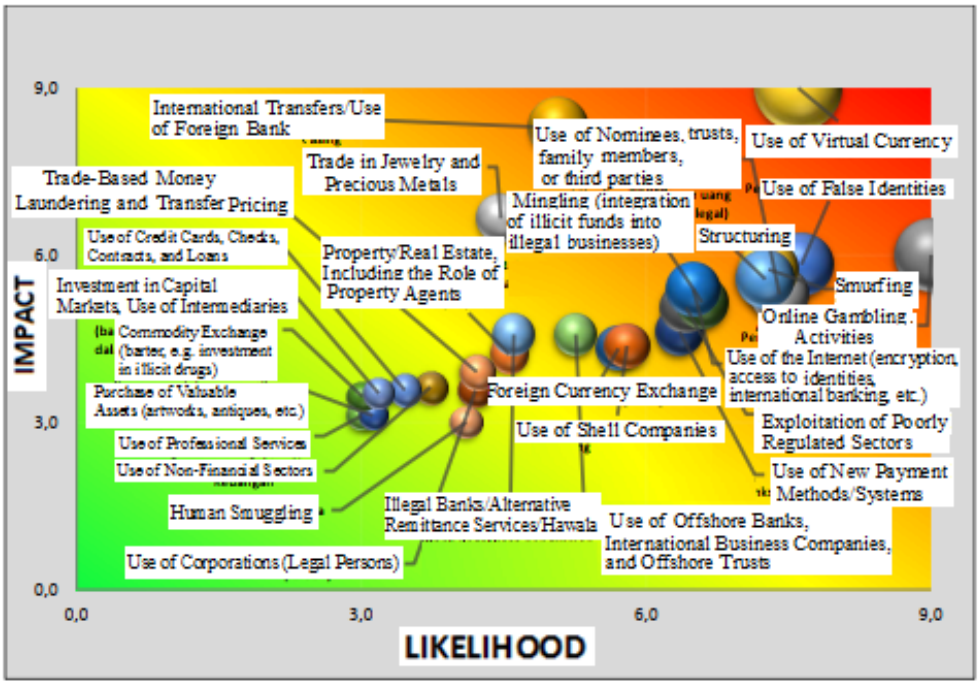

Figure 12 Risk Level of ML from Cybercrime Based on ML Typology

8. Money Laundering Risk Level of Cybercrime Proceeds Based on Transaction Patterns

Based on transaction patterns, the transaction patterns assessed as posing a high money laundering (ML) risk arising from cybercrime are fund transfers and cash withdrawals/deposits. Internet banking/mobile banking, purchases of crypto-asset products, virtual accounts, and the use of new payment instruments (electronic money and electronic wallets) are assessed as posing a medium ML risk.

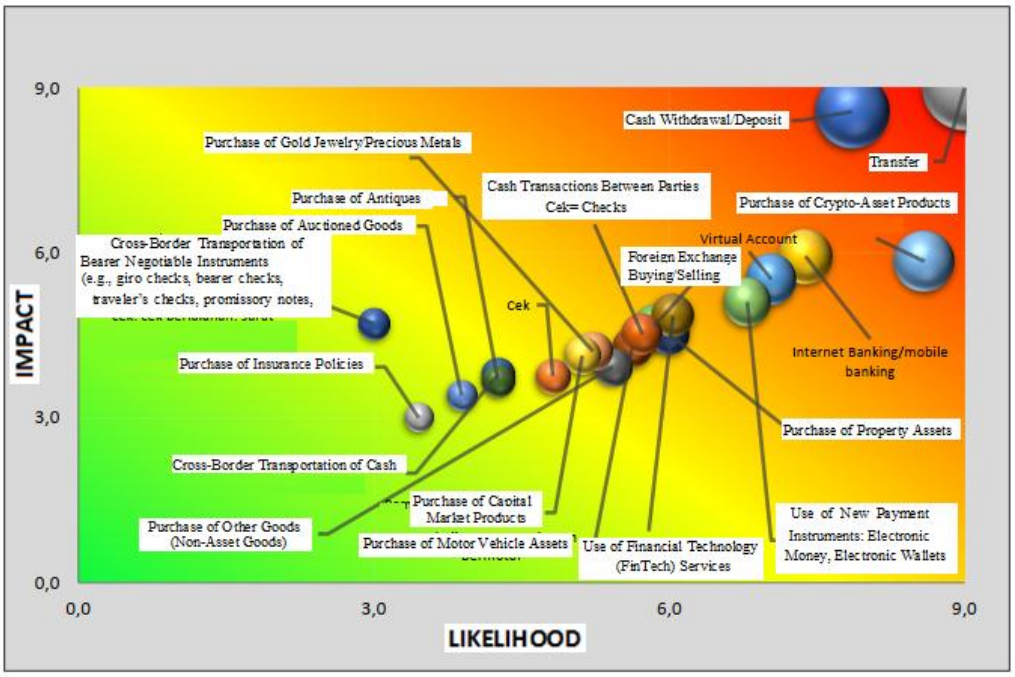

Figure 13 ML Risk Level from Cybercrime Based on Transaction Pattern

9. Potential Risk of Destination, Source, and Transit Countries for Money Laundering Proceeds from Cybercrime

As discussed in the previous section, cybercrime does not recognize geographical or territorial boundaries. Therefore, respondents were asked to identify countries that have the potential to serve as destination countries, source countries, and transit countries for money laundering proceeds derived from cybercrime. The results are as follows:

Table 3 Potential Risk of Destination, Origin, and Transit Countries for ML Proceeds from Cybercrime

No.	Destination Country for ML Fund Transfers from Indonesia	Source Country of ML Fund Transfers to Indonesia	Transit Country for ML Funds to Indonesia	Transit Country for ML Funds from Indonesia
1	Singapore	United States	Singapore	Singapore
2	United States	People's Republic of China	Hong Kong	Malaysia
3	Hong Kong	India	People's Republic of China	United States

The reasons respondents identified the above countries as having the potential to serve as source, destination, and transit countries for money laundering proceeds derived from cybercrime are as follows:

Singapore

- Regional financial hub with relatively lax banking regulations and openness to foreign capital
- Geographically close to Indonesia
- Has well-developed digital financial services
- Have no regulation requiring companies to disclose beneficial ownership
- Legalizes gambling. In general, proceeds from cybercrime are used for gambling-related offenses
- Cybercrime originating from Singapore uses nominees/shell companies in Indonesia

United States

- The largest economy in the world
- Highly developed capital markets
- Very high level of internet usage
- Serves as a hub for various online platforms and digital financial services

Hong Kong

- A major regional financial center
- Strong banking system and advanced financial infrastructure
- Legalizes gambling. In general, cybercrime proceeds are used for gambling-related offenses
- Based on banks' experience, fictitious companies are used for fictitious invoice payments

People's Republic of China

- Has relatively lax data privacy regulations and serves as a hub for various online platforms and digital financial services

India

- There are extensive business and economic relationships between India and Indonesia, including fund transfers, investment, and trade

Malaysia

- A developing financial sector with fairly advanced banking facilities
- Geographically close to Indonesia

Figure 14 Reasons Respondents Identified Countries with Potential as Sources, Destinations, or Transit Points for ML Proceeds from Cybercrime

B. Terrorist Financing Risk Level

Based on the data collected and field findings, only a risk assessment of money laundering (ML) arising from cybercrime could be conducted. At present, a terrorist financing

(TF) risk assessment cannot yet be carried out, as during the study period (2020–2024) no TF cases were identified in which the funding originated from cybercrime. A TF case funded through cybercrime was previously identified in 2012 (the CAHYA FITRIANTA case, pursuant to Court Decision No. 113/PID/2013/PT.DKI), in which the defendant financed terrorism by hacking an investment website. According to the National Risk Assessment (NRA) on Terrorist Financing and Proliferation Financing of Weapons of Mass Destruction (2021), terrorist financing methods in Indonesia during the period 2016–2020 were generally conducted through legal or seemingly legal means (INTRACT, 2021). Examples include private sponsorship (terrorist financiers/fundraisers), misuse of donation collections through mass organizations, and legitimate business activities.

Although no further TF cases arising from cybercrime have been identified in Indonesia, this does not mean that terrorists or terrorist organizations do not exploit cyberspace for financing or other activities. For example, weapons used in the 2015 Paris and 2016 Munich attacks were allegedly obtained through the dark web (United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institute, 2024). In addition, cyberspace is widely used for communication, propaganda, and recruitment (Malik, 2018; Australian Strategic Policy Institute, 2021). According to Levi West, Director of Terrorism Studies at Charles Sturt University Graduate School for Policing and Security, terrorists have not yet widely shifted toward cyber-based financing, but have already extensively used cyberspace for recruitment (Australian Strategic Policy Institute, 2022).

In 2023, the Global Terrorism Index identified Burkina Faso (West Africa) as the country with the highest terrorism impact, followed by Israel (West Asia) and Mali (West Africa). Following the decline of ISIS/ISIL, there has been a shift in the global terrorism landscape toward the West African region. In the context of the Sahel region—the intersection between Sub-Saharan Africa and the Middle East—poorly monitored cyberspace and weak mechanisms governing cross-border cash flows are believed to accelerate the growth of jihadist cells in West African countries in the future, or enable existing groups to further consolidate power by expanding their networks and recruitment bases. It has also been noted that cyber fraud may become an important source of funding for jihadist groups in the region (Australian Strategic Policy Institute, 2022). The FATF (2020) also highlighted that the COVID-19 pandemic increased cybercrime such as fraud, which may affect online terrorist financing, including schemes disguised as COVID-19 donations.

Technological developments beyond cyberspace are also exploited by terrorists or terrorist financiers to facilitate terrorist financing, including the use of crypto-assets/virtual assets[3]. Prior to the widespread use of crypto-assets, internet-based money transfer services had already been used by terrorists or terrorist financiers to move funds (Sa'diyah, 2017). At the international level, Al-Qaeda has been reported to raise funds through crypto-assets (U.S. Immigration and Customs Enforcement, 2020).

Cases of alleged terrorist financing through cyber fraud have been identified in the United States, where ISIS facilitators sold purported FDA-approved N95 masks, which in fact did not meet U.S. Food and Drug Administration standards (U.S. Immigration and Customs Enforcement, 2020). Although terrorist financing through cybercrime has not reoccurred in Indonesia, such cyber-fraud-based TF cases abroad underscore the importance of continued vigilance, particularly regarding the use of cyberspace and financial technology in terrorist financing.

4.2. Emerging Threats

Emerging threats of money laundering (ML) and terrorist financing (TF) arising from cybercrime, as identified by respondents, include the following:

1. Misuse of Artificial Intelligence

   Artificial Intelligence (AI) technology is increasingly being used today. AI technology that may be exploited by criminals includes generative AI, such as creating images or videos that resemble real individuals, as well as replicating human voices, in order to deceive security systems used by financial service providers.

2. Misuse of E-Wallets

[3] The FATF uses the term Virtual Assets, whereas Indonesia adopts the term Crypto Assets, as stipulated in Minister of Trade Regulation No. 99 of 2018 on the General Policy for the Implementation of Crypto Asset Futures Trading. Crypto Assets in Indonesia differ from the FATF's concept of Virtual Assets in that Crypto Assets are not permitted to be used as a means of payment. However, for the purposes of this study, Crypto Assets may be regarded as equivalent to Virtual Assets as defined by the FATF.

Electronic wallets or e-wallets are essentially technologies designed to facilitate payments; however, they are misused by criminals as tools for storing funds and transferring funds.

3. Use of Coin-Mixing Services (Coin Mixers)

Coin-mixing services can obscure the trail of crypto-assets by mixing crypto-assets and redistributing them, thereby making the funds appear legitimate.

4. Distribution of Links/Files Containing Malware or for Attempted Data Takeover

This modus operandi has become increasingly prevalent in recent years, involving the transmission of messages through messaging applications containing links or files that carry malware or can install applications capable of stealing user data.

5. Use of Private Wallet Addresses

Crypto-assets enable transactions not only through physical crypto-asset traders but also through peer-to-peer transactions. The use of private wallet addresses can make it difficult for investigators to trace funds.

6. Exploitation of Web3 and Crypto-Assets

Figure 15 Fraud Scheme Using Crypto Assets

Source: Wu et al. (2023)

Web3 represents the latest generation of the internet, utilizing blockchain technology to bring users closer to their digital assets and identities. Crypto-assets are central to this Web3-

based economy. The lack of uniform blockchain regulation worldwide enables Web3 to be exploited by criminals. In the crypto-asset market, fraudsters take advantage of the pseudonymous nature of crypto-assets to conduct untraceable crypto-asset fraud and attempt to deceive investors in order to obtain illicit gains.

4.3. Typologies and Case Studies

This section discusses case studies based on court decisions in Indonesia related to cybercrime and money laundering (ML) (seven cases), as well as one case from Australia. From the cases described below, the following conclusions can be drawn:

1. Offenders continue to use bank accounts to store and transfer funds.
2. Offenders continue to purchase physical goods to conceal the origin of criminal proceeds.
3. Offenders utilize physical crypto-asset traders, both domestic and foreign, to hide and disguise the origin of criminal proceeds.

Case 1

Predicate Offence: Illegal Access

Based on Court Decision No. 355/Pid.Sus/2021/PN Dps

I GEDE ADNYA SUSILA worked as a Credit Marketing Officer at BPR Lestari, Benoa Branch, Denpasar. I MADE DARMAWAN was a customer of PT BPR Lestari, Benoa Branch. The incident began around 18 June 2020, when the wife of I MADE DARMAWAN was contacted by I GEDE ADNYA SUSILA, who informed her that he would visit their stall to meet. Subsequently, I GEDE ADNYA SUSILA informed them that there was a banking service product that needed to be activated, namely the LESTARI MOBILE application, and offered to install the application on I MADE DARMAWAN's mobile phone. I MADE DARMAWAN then handed over his mobile phone, and I GEDE ADNYA SUSILA downloaded the Lestari Mobile application and requested I MADE DARMAWAN's email address, which was provided. After installing the application, I GEDE ADNYA SUSILA returned the mobile phone to I MADE DARMAWAN, stating that the application had been activated. However, I MADE DARMAWAN did not know whether the mobile banking service had actually been activated, as no transaction was attempted at that time.

At the same time, I GEDE ADNYA SUSILA also downloaded the LESTARI MOBILE application onto his own mobile phone. After completing the download, I GEDE ADNYA SUSILA proceeded to carry out the activation process simultaneously on I MADE DARMAWAN's mobile phone and his own mobile phone, by entering customer data including

the account number, phone number, and email address. Subsequently, I MADE DARMAWAN, as the customer, received an OTP code via email and SMS, and I GEDE ADNYA SUSILA input the OTP code into his own mobile phone, while no OTP code was entered on I MADE DARMAWAN's mobile phone. Shortly thereafter, I MADE DARMAWAN received a confirmation call from the LESTARI MOBILE activation service, and at that moment I GEDE ADNYA SUSILA allowed him to respond to the activation confirmation. Next, I GEDE ADNYA SUSILA created a mobile banking PIN to be used for transactions. He then returned I MADE DARMAWAN's mobile phone, stating that LESTARI MOBILE had been activated, whereas in fact, it was not activated. Instead, the activated one was on I GEDE ADNYA SUSILA's mobile phone. Thereafter, I GEDE ADNYA SUSILA used Lestari Mobile belonging to I MADE DARMAWAN, installed on his own mobile phone, to conduct fund transfer transactions from I MADE DARMAWAN's bank account to several accounts, including I GEDE ADNYA SUSILA's own account, with the following details:

1. June 2020: There were three transactions with a total amount of IDR 150,000,000, transferred via Mobile Banking to BCA Account No. 0380658160 in the name of RAJIB ARSAD GANI.
2. July 2020: There were eight transactions with a total amount of IDR 277,100,000, transferred via Mobile Banking to BCA Account No. 0380658160 in the name of RAJIB ARSAD GANI.
3. August 2020: There were fourteen transactions with a total amount of IDR 453,050,000, transferred via Mobile Banking to BCA Account No. 0380658160 in the name of RAJIB ARSAD GANI.
4. September 2020: There were three transactions with a total amount of IDR 96,500,000, transferred via Mobile Banking to BCA Account No. 0380658160 in the name of RAJIB ARSAD GANI.
5. October 2020: There were eleven transactions with a total amount of IDR 425,000,000, consisting of seven (7) transactions transferred via Mobile Banking to BCA Account No. 0380658160 in the name of RAJIB ARSAD GANI, with a total amount of IDR 280,000,000; and four (4) transactions transferred via QR Mobile Banking to BPR Lestari Account No. 0100050466 in the name of ADNYA SUSILA, with a total amount of IDR 145,000,000.

6. November 2020: There were two transactions with a total amount of IDR 53,500,000, transferred via QR Mobile Banking to BPR Lestari Account No. 0100050466 in the name of ADNYA SUSILA.

The total amount of transferred funds was IDR 1,455,150,000. All of these funds were used by I GEDE ADNYA SUSILA to participate in online gambling activities and to cover his personal expenses.

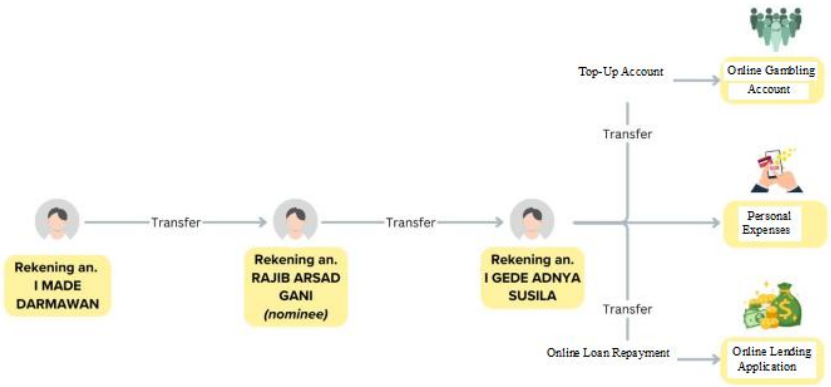

Figure 16 Overview of the I Gede Adnya Susila Case

The defendant's actions, as regulated and subject to criminal sanctions, violate Article 32 paragraph (2) in conjunction with Article 48 paragraph (2) of the Law of the Republic of Indonesia No. 19 of 2016 on Amendments to Law of the Republic of Indonesia No. 11 of 2008 concerning Electronic Information and Transactions, as well as Article 3 of Law of the Republic of Indonesia No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering. For these offenses, the defendant was sentenced to five (5) years' imprisonment and a fine of IDR 2,000,000,000.00 (two billion rupiah), with the stipulation that failure to pay the fine shall be substituted by a term of confinement of three (3) months.

Case 2

Predicate Offense: Pornography and Online Gambling

Based on Decision No. 345/PID.SUS/2020/PT BDG

Reynaldi Marcellino, also known as Lim Sui Liong alias Ali, was the owner of a website containing pornographic content under the domain https://zonalendir.net/. The pornographic content hosted on the website did not solely involve adult pornography but also involved children as objects. The website also displayed advertisements, totaling 28 content placements,

consisting of 22 pornographic forums with a total of 917,559 threads and 145,359 registered members, as well as six (6) additional forums comprising 34,043 threads and 2,630 members.

Investigators' findings revealed the involvement of another individual, Suwarno alias Eno. The defendant Reynaldi and Eno agreed to engage in financial cooperation related to the provision of websites hosting pornographic content and online gambling advertisements. This cooperation included the rental of servers through the website www.ditusuk.in, as well as the creation of a new website under the domain http://terselubung.us.

. Defendant Reynaldi Marcellino obtained stories, photographs, and videos containing pornographic elements or violating public morality by sourcing them from www.semprot.com, which is known as one of the largest forums in Indonesia hosting pornographic content and facilitating online prostitution. The pornographic or immoral content could be accessed freely by any visitor without requiring prior membership.

The profit obtained from all forum websites owned by the defendant from their initial operation until the court's decision amounted to approximately IDR 100,000,000 (one hundred million rupiah). These proceeds were used by the defendant to cover website operational costs, purchase mobile phones, computers, laptops, and to meet daily living expenses. In addition, the defendant purchased one (1) unit of a black metallic Wuling car, model year 2017, with vehicle registration number F-1015-BA. The defendant's actions in purchasing goods using proceeds derived from advertisements placed on pornographic-content websites constitute acts of spending assets derived from criminal activity, and demonstrate efforts to conceal or disguise the origin of assets derived from criminal proceeds.

The defendant was proven to have violated Article 45 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, in conjunction with Article 55 paragraph (1) point 1 of the Indonesian Criminal Code (KUHP), Article 3 of Law No. 8 of 2010 on the Prevention and Eradication of the Crime of Money Laundering, Law No. 8 of 1981 on Criminal Procedure, and other relevant laws and regulations. The sentence imposed on Reynaldi Marcellino alias Lim Sui Liong was eight (8) years' imprisonment, reduced by the period of temporary detention already served, with an order that the defendant remain in custody, and a fine of IDR 1,000,000,000 (one billion rupiah), subsidiary to six (6) months of confinement in the event the fine is not paid.

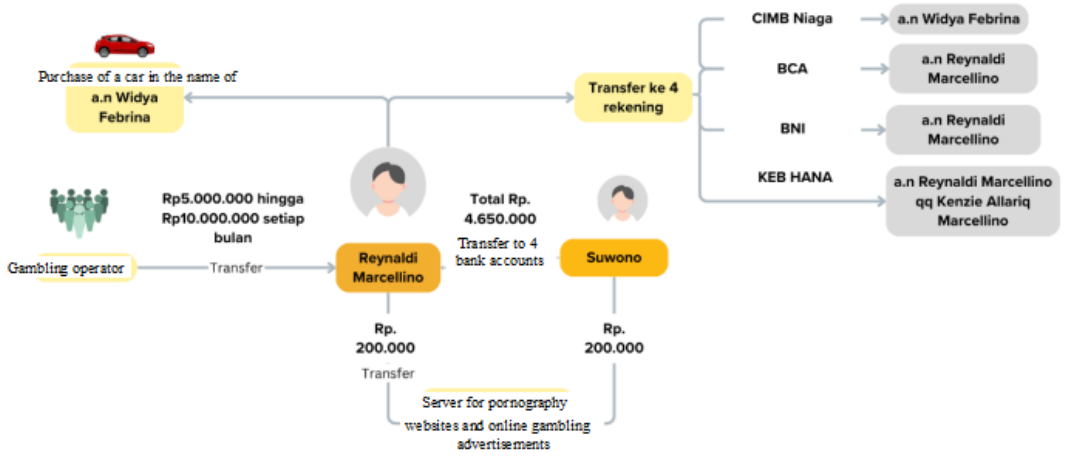

Figure 17 Overview of the Reynaldi Marcellino alias Lim Sui Liong alias Ali Case

Case 3

Predicate Crime: Online Gambling

Based on Court Decision No. 94/Pid.Sus/2024/PN Jkt.Utr

Indradi, also known as Indradi Halim, also known as OOW, son of Bahtiar Halim, served as a marketing team leader on the online football betting website www.egogoro.com, which provided online sports betting, slot games, and casino gambling. The defendant played a role in managing the website and coordinating employees to recruit or persuade others to participate in gambling activities on the website. Before starting to gamble, players were required to deposit funds into their online gambling accounts. Employees recruited by the defendant were tasked with assisting the deposit process, including the disbursement (withdrawal) of funds conducted by players. Their deposit funds were collected and held in the following accounts:

1. BCA Account No. 0403062950 in the name of Dieva Bunaya, which was obtained by the defendant through purchase from a third party;
2. BNI Account No. 1438849085 in the name of Caesar Ivantyo, who was a sales marketing employee of the website www.egogoro.com;
3. BRI Account No. 721001012690536 in the name of Caesar Ivantyo;
4. Mandiri Account No. 60011499815 in the name of Caesar Ivantyo;
5. Mobile credit deposit to Telkomsel number 081283879894; and
6. DANA e-wallet deposit to Smartfren number 08886392504.

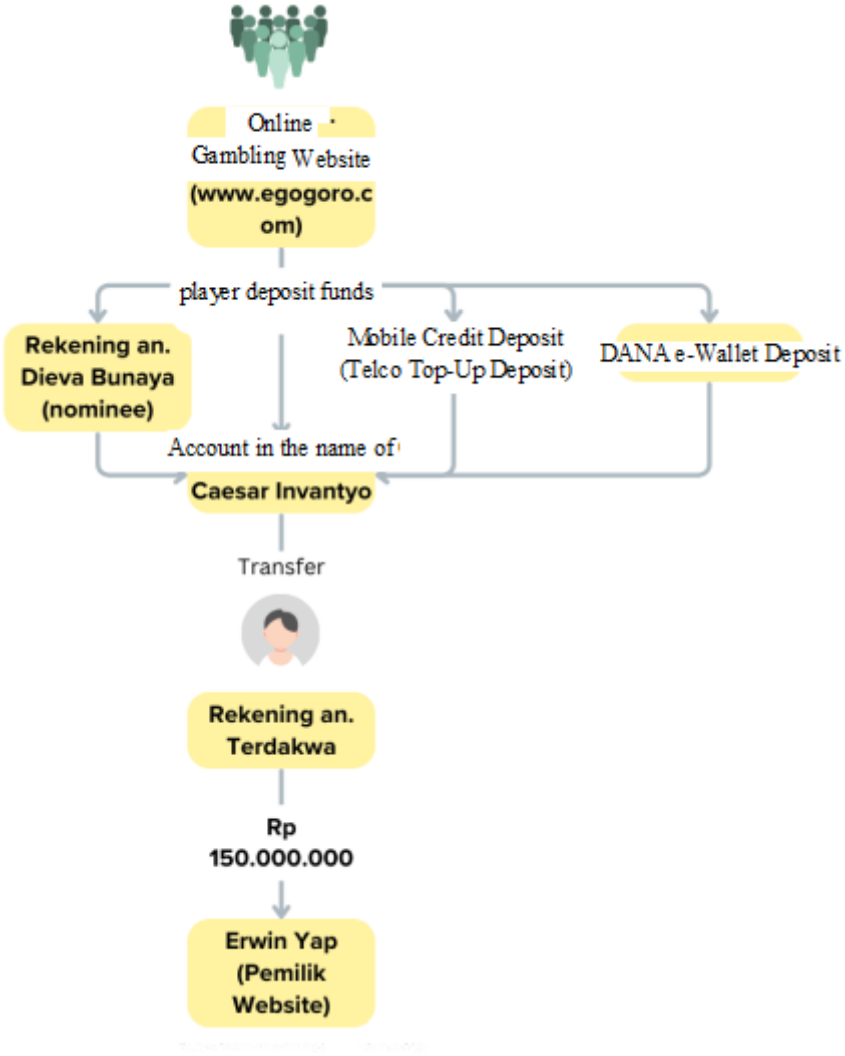

Figure 18 Overview of the Indradi alias Indradi Halim alias OOW Case

The operation of the online gambling website generated a turnover of IDR 300,000,000.00, with profits amounting to IDR 150,000,000.00. These profits were subsequently transferred by Caesar Ivantyo to the defendant's bank account and were then forwarded to Erwin Yap (a Singaporean national), who is the owner of the website www.egogoro.com. The defendant was legally and convincingly proven guilty of committing a criminal offense by participating jointly, intentionally and without authority, in distributing and/or transmitting and/or making accessible Electronic Information and/or Electronic Documents containing gambling content, as well as placing, transferring, diverting, spending, paying, granting, entrusting, carrying funds abroad, converting, exchanging into currency or securities, or committing other acts involving assets which he knew or reasonably should have suspected were proceeds of a criminal offense, with the purpose of concealing or disguising

the origin of such assets. The defendant was sentenced to imprisonment for 1 (one) year and 6 (six) months and ordered to pay a fine of IDR 75,000,000.00 (seventy-five million rupiah).

Case 4

Predicate Crime: Phishing

Based on Court Decision No. 511/Pid.Sus/2023/PM JKT.SEL

Muhammad Fauji Alfariz (Defendant I), through a Facebook account named Kristen, obtained approximately two million Hotmail-domain email addresses, as well as Remote Desktop Protocol (RDP) account credentials and passwords, SMTP access, and cPanel access from a Facebook group called SIXTEEN MARKET. Using the obtained email addresses, Google SMTP, RDP, and cPanel access, Defendant I initiated phishing activities, having previously prepared the phishing website scripts himself. Emails sent by the defendant to prospective victims appeared to be legitimate emails from the Coinbase platform, containing messages stating that the recipient's Coinbase account had encountered a problem and required re-verification. One of the victims was Melody June Royalty, with the email address melody_sturgill@hotmail.com. The victim clicked a fraudulent button that redirected her to a phishing website created by Defendant I. On that page, the victim entered the username and password of her Coinbase account, which contained her digital currency holdings. The account credentials were stored in a so-called pandora box, which Defendant I later accessed via RDP.

After gaining access to the victim's Coinbase account, Defendant I transferred the victim's Bitcoin and Ethereum to a Binance wallet belonging to Fahri Fauzi (Defendant II) and to several Indodax wallets controlled by Defendant I, in five transactions. The total value of the transferred digital assets, when converted into fiat currency at the time, amounted to approximately IDR 19,330,191,926.00. Defendant I also provided USDT digital assets to Defendant II as compensation for lending his Binance wallet, which at the time was equivalent to approximately IDR 2,500,000,000.00 in fiat currency. Meanwhile, the Indodax wallets controlled by Defendant I were registered under the names Muhammad Fauji Alfariz, Ahmad Sururi, Ahmad Kumaedi, and Muhammad Rizki. The digital assets under Defendant I's control were subsequently converted into fiat currency in Indonesian rupiah. The funds were used to purchase various assets (including a house, clothing, bags, watches, and luxury vehicles), services (home renovations and life insurance), and to make transfers to family members (mother, wife, and parents-in-law). Defendant II likewise converted the digital assets under his

control into rupiah, which were used to purchase assets (a house, a vape shop, and vehicles), services (Umrah pilgrimage and vehicle modification), and to make transfers to his wife.

Defendants I and II were legally and convincingly proven guilty of aiding and abetting, intentionally and unlawfully, the transfer or transmission of Electronic Information and/or Electronic Documents to electronic systems belonging to unauthorized parties, resulting in losses to others, as well as committing money laundering offenses. Each of the defendants was sentenced to 6 (six) years of imprisonment and ordered to pay a fine of IDR 2,000,000,000.00 (two billion rupiah).

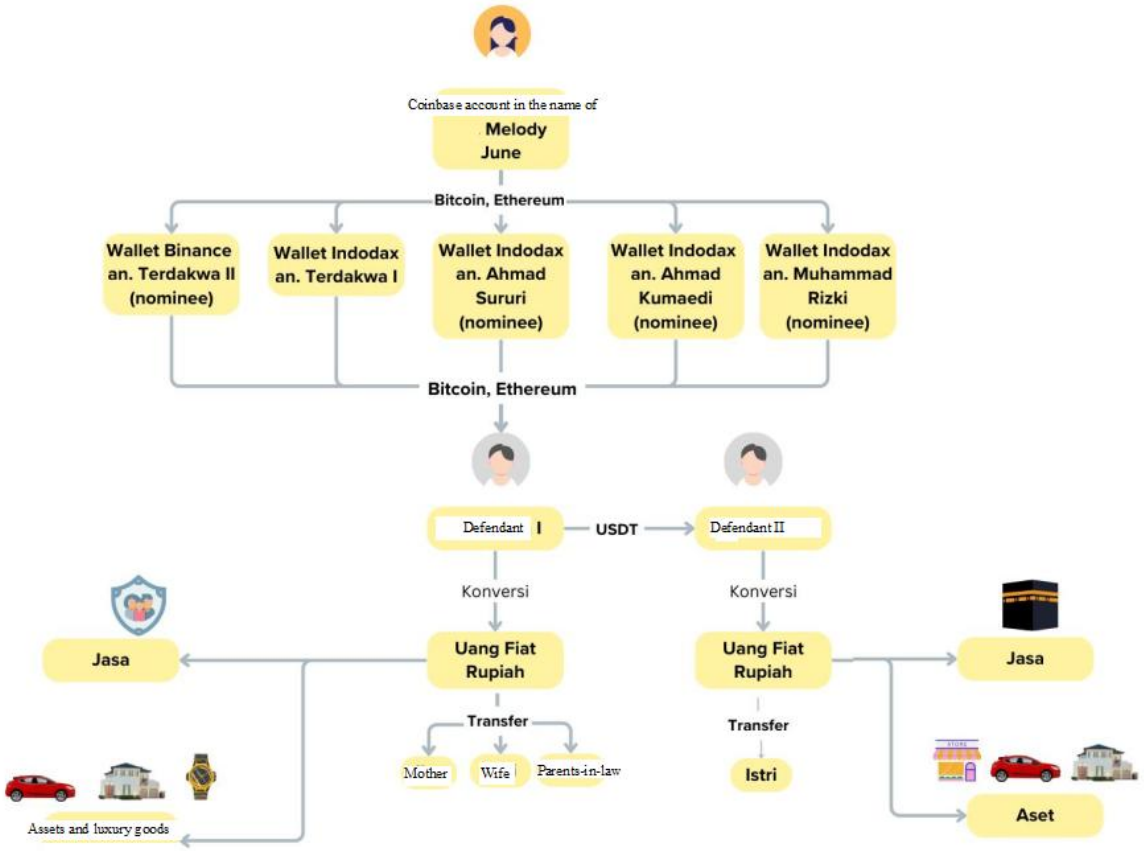

Figure 19 Overview of the Muhammad Fauji Alfariz and Fahri Fauzi Case

Case 5

Predicate Crime: Fraud

Based on Decision No. 205/PID.SUS/2021/PT.DKI

Drelia Wangsih used her personal Facebook account to offer gold bullion purportedly issued by PT Antam Tbk at relatively low prices. The offers were made through livestreams, during which the defendant read out and displayed updated Antam gold price lists and showed gold bars that she claimed to be selling, stating that the gold was always available and ready for delivery. The gold was actually purchased by the defendant from retail gold shops, namely Toko Emas Mulia ITC Cempaka Emas Mega Grosir, Toko Emas Singa Emas, and gold shops at Koja Market, North Jakarta. The gold was initially delivered to buyers, causing them to feel confident and interested in making repeat purchases. However, the defendant did not have a license to sell gold. The defendant provided a bank account in the name of Rohimah to facilitate payment transactions for buyers. For subsequent orders involving larger amounts of money, however, the defendant failed to deliver the ordered gold, even though the buyers had transferred the payment. The transferred funds were not returned by the defendant.

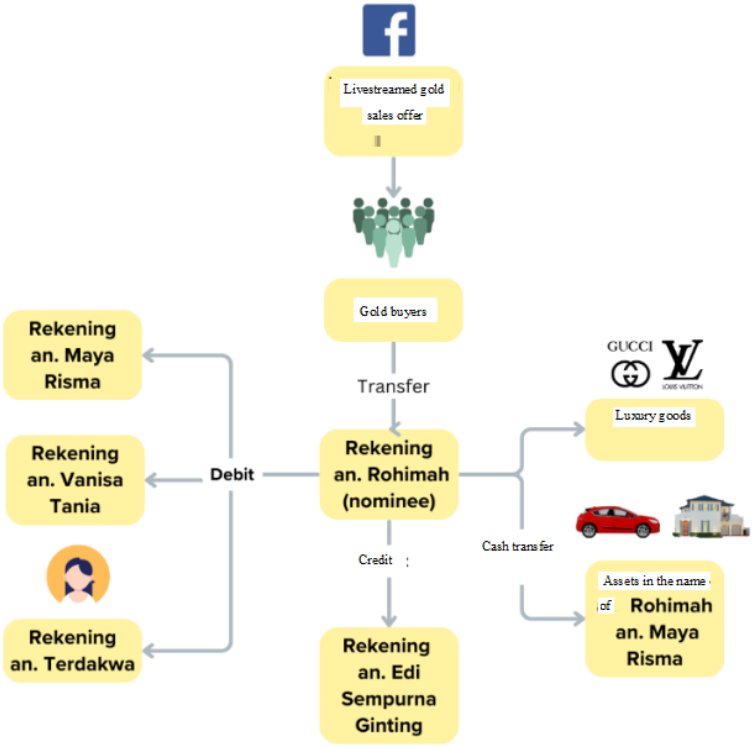

Figure 20 Overview of the Drelia Wangsih Case

The funds received as payment for the gold, which were deposited into the bank account in the name of Rohimah, were subsequently transferred to the defendant's bank account. The transactions carried out by the defendant using the proceeds included the following:

1. Purchasing luxury goods bearing the brands Louis Vuitton, Gucci, Christian Dior, and Off-White;
2. Debit transactions from the bank account in the name of Rohimah to the bank accounts in the names of Maya Risma, Vanisa Tania, and the defendant;
3. Credit transactions from the bank account in the name of Rohimah to the bank account in the name of Edi Sempurna Ginting; and
4. Purchases of land, buildings, and vehicles, both in cash and on credit.

The defendant was declared lawfully and convincingly guilty of committing the criminal offenses of fraud and money laundering. The defendant was sentenced to imprisonment for a term of 4 (four) years and fined IDR 500,000,000.00 (five hundred million rupiah).

Case 6

Predicate Crime: Fictitious Sale of Medical Devices via a Website

Based on Court Decision No. 492/Pid.Sus/2019

Mr. James Bangun (fugitive/subject to wanted list) contacted Aldaf Risia (Defendant I) and requested that he procure a bank account using false identity data (nominee) to receive payments from fictitious online transactions involving medical devices through the website www.bastmed.com, owned by Mr. James Bangun. Defendant I was promised a fee equal to 20% of the funds received in the account. Subsequently, Defendant I contacted Jamaluddin Garinging (Defendant II) to obtain a nominee bank account in accordance with Mr. James Bangun's request. Defendant II was likewise promised a fee of 20% of the funds deposited into the account. Defendant II succeeded in obtaining a nominee bank account by purchasing it from Mr. Adi Sucipto for approximately IDR 3,000,000.00, and acquired a BNI bank passbook and ATM card associated with account number 0721835260 in the name of Mashuri. Defendant II then informed Defendant I, who forwarded this information to Mr. James Bangun.

Mr. James Bangun later contacted Defendant I again, informing him that a prospective buyer would make a payment under the name Andrea Martinez to Bank BNI. Defendant I was

instructed to reply to the prospective buyer's email using the address sales@bastmed.com regarding the purchase of two units of the VERSA-TRAC Lumbar Retractor Master Set for a total price of USD 8,400. Following the price agreement, Defendant I edited the invoice and company profile to display "Bastmed formerly known as MASHURI" in order to enhance the victim's trust.

Defendant II then informed Defendant I that funds in the amount of USD 8,400, equivalent to IDR 123,302,480.00, had been transferred by Andrea Martinez into the nominee account. From this amount, Defendant II received a commission of 20%, amounting to IDR 24,000,000.00, while the remaining balance was transferred by Defendant II to Defendant I's BCA bank account under the name Aldaf Risia, account number 0080852983, in several stages: IDR 45,000,000.00 via teller deposit at BCA KCP Nagoya; IDR 47,250,000.00 via teller deposit at BCA KCP Penuin, Batam; and IDR 9,000,000.00 via Bank Mandiri mobile banking. Thereafter, Defendant I transferred the funds received from Defendant II to Mr. James Bangun's BCA account number 8200283563, after deducting IDR 16,000,000.00 as his commission. Consequently, the amount transferred to Mr. James Bangun totaled IDR 74,000,000.00.

Defendant I and Defendant II were declared lawfully and convincingly guilty of committing the criminal offenses of fraud and conspiracy to commit money laundering, namely transferring assets known to be the proceeds of a criminal offense with the intent to conceal or disguise their true origin. The defendants were each sentenced to 1 (one) year and 8 (eight) months' imprisonment and fined IDR 50,000,000.00 (fifty million rupiah).

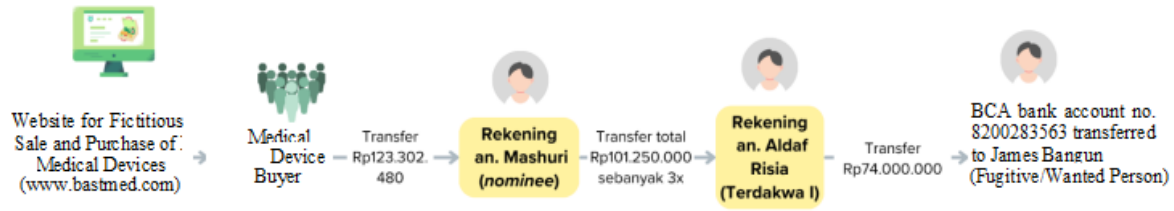

Figure 21 Overview of the Aldaf Risia and Jamaluddin Garinging Caseq

Case 7

Predicate Offence: Fraud and Embezzlement in Robot Trading Investment

Based on Judgment Number 24/Pid-Sus/2023/PT.DKI

The defendant Hendry Susanto collaborated with Dylan Velio to establish a robot trading business. Hendry Susanto acted as the founder and director of PT FSP Akademi Pro, while Dylan Velio acted as the founder of PT Lotus Global Buana. PT FSP Akademi Pro functioned as the seller of the Fahrenheit trading robot application, while PT Lotus Global Buana acted as the trading robot broker.

The registered business license is stated in the Risk-Based Business Licensing Attachment of PT FSP Akademi Pro No. 12770007304210003, registered as Financial Recording Software, with three product trademarks: Catat Basic, Catat Pro, and Catat Premium. The violation committed by the defendant was conducting business activities not in accordance with the registered business license. The dissemination of sales information for the Fahrenheit Robot Trading was conducted through social media by uploading videos to YouTube, TikTok, Instagram, Twitter, and Facebook, as well as distributing digital flyers via WhatsApp story uploads created by Inton Luando Yohanes.

Meanwhile, PT Lotus Global Buana, acting as a broker for Fahrenheit robot trading members, did not possess a license from Commodity Futures Trading Regulatory Agency (BAPPEBTI) for operating as a Futures Exchange, Futures Clearing Institution, Futures Broker, Futures Advisor, Futures Fund Management Center, nor did it hold registration certificates as a Futures Trader, Prospective Physical Crypto Asset Trader, or any other form of licensing under the name of PT Lotus Global Buana. The business scheme used by the defendants was Multi-Level Marketing (MLM). The Fahrenheit robot trading investment scheme promised returns of 1 percent per day, or 20–25 percent per month. Each member was allowed to have two or more accounts using the same identity or email address.

The robot trading accounts used were verified using account IDs and passwords on the MetaTrader 4 (MT4) application. The fee to obtain the Fahrenheit robot or trading script was sold at 10 percent of the investment value, using an exchange rate of IDR 15,000 per USD, and packaged into the following investment tiers:

1. **Newbie**: USD 500 or equivalent to IDR 7,500,000, robot value 10% or USD 50. Trading profit distribution: 50% for investors and 50% for the company.
2. **Premium**: USD 1,000 or equivalent to IDR 15,000,000, robot value 10% or USD 100. Trading profit distribution: 60% for investors and 40% for the company.

3. **Professional**: USD 5,000 or equivalent to IDR 75,000,000, robot value 10% or USD 500. Trading profit distribution: 70% for investors and 30% for the company.
4. **Expert**: USD 10,000 or equivalent to IDR 150,000,000, robot value 10% or USD 1,000. Trading profit distribution: 75% for investors and 25% for the company.
5. **Advance**: USD 25,000 or equivalent to IDR 375,000,000, robot value 10% or USD 2,500. Trading profit distribution: 80% for investors and 20% for the company.
6. **Legend**: USD 50,000 or equivalent to IDR 750,000,000, robot value 10% or USD 5,000. Trading profit distribution: 90% for investors and 10% for the company.

The defendant promised three types of benefits to members who invested in the Fahrenheit Robot Trading, namely: profit sharing, downline trading profits, and group sales bonuses based on sales rankings within the MLM scheme. Members who successfully recruited downline members were promised various additional rewards such as precious metals, cars, laptops, mobile phones, motorcycles, and commission bonuses, which in reality were derived from funds deposited by the members themselves, rather than from actual trading profits.

The profit distribution by network level within the MLM scheme promised by PT FSP Akademi Pro was as follows:

1. Level 1: 50%
2. Level 2: 20%
3. Level 3: 15%
4. Level 4: 10%
5. Level 5: 5%.

The witnesses Maria Fransiska, David, and the defendant Hendry Susanto did not possess any licenses, certifications, or adequate expertise as exchange providers. Instead, they merely controlled accounts used to hold investment funds deposited by members of PT FSP Akademi Pro. The defendant used investment funds originating from members to finance his business activities, pay company operational expenses, and distribute profits and bonuses to members. This means that members' deposited funds were recycled through a Ponzi scheme.

The chronology of the scam carried out by the defendant Hendry Susanto began with the creation of a video uploaded to the social media accounts of PT FSP Akademi Pro, announcing an alleged regulatory adjustment by the government. The defendant claimed that the government required robot trading providers to obtain trading licenses for robot trading services. This claim was used by the defendant as a justification for PT FSP Akademi Pro to

suspend trading activities and halt investment withdrawals by members. On 25 February 2022, the Fahrenheit Robot Trading system ostensibly resumed trading activities; however, members were still unable to withdraw funds and were promised that withdrawals of investment capital and trading commissions would be possible on 7 March 2022. This fictitious trading activity was intended to convince members that PT FSP Akademi Pro was making efforts to comply with new government regulations, so that members would not panic or realize that they were being defrauded.

From 25 February 2022 to 7 March 2022, investment losses occurred among Fahrenheit robot trading members, resulting in the total depletion of members' capital, engineered to appear as though it was caused by a margin call. The defendants Hendry Susanto and Dylan Velio deliberately created these losses to appear as a consequence of legitimate trading transactions, whereas in reality the transactions were entirely fictitious, and the margin calls were intentionally engineered as an exit plan.

Based on audit results, 1,449 members reported losses out of approximately 20,000 Fahrenheit robot trading members. It was determined that these 1,449 members suffered total losses amounting to approximately IDR 358,297,322,001(three hundred fifty-eight billion two hundred ninety-seven million three hundred twenty-two thousand and one rupiah).

According to the opinion of an Information Technology and Electronic Transactions (ITE) expert, Dr. Ronny, S.Kom, M.Kom, M.H., the trading robot marketed by PT FSP Akademi Pro was illegal because it had not obtained approval from the Government, particularly from BAPPEBTI and the Financial Services Authority (OJK). The investment offering by Fahrenheit, which promised high potential returns, was capable of influencing the public to participate and join as members. However, in electronic trading transactions, there is always an equal possibility of profit and risk of loss. Moreover, it was proven that Fahrenheit marketed a trading robot that conducted fictitious transactions and merely operated a Ponzi scheme as its business model.

The actions carried out by PT FSP Akademi Pro, involving the defendants Hendry Susanto, Dylan Velio, and Ferry Nando, constitute criminal acts as regulated and punishable under Article 45A paragraph (1) in conjunction with Article 28 paragraph (1) of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), in conjunction with Article 55 paragraph (1) subparagraph 1 of the Criminal Code (KUHP), and under the Second Indictment, Article 3 in conjunction with Article 10 of Law No. 8 of 2010 on the Prevention and Eradication of Money Laundering. The

defendants were found to have concealed the proceeds of crime by using companies under their control. They were also proven to have engaged in criminal conspiracy with other parties serving as witnesses to provide nominee accounts used to place and store proceeds of criminal activities.

The defendants were legally and convincingly proven guilty of intentionally and unlawfully disseminating false and misleading information that caused losses to consumers in electronic transactions, as well as committing money laundering offenses. The sentence imposed on the defendant was 10 (ten) years' imprisonment and a fine of IDR 3,000,000,000.00 (three billion rupiah), with the provision that if the fine is not paid, it shall be substituted by 6 (six) months' imprisonment.

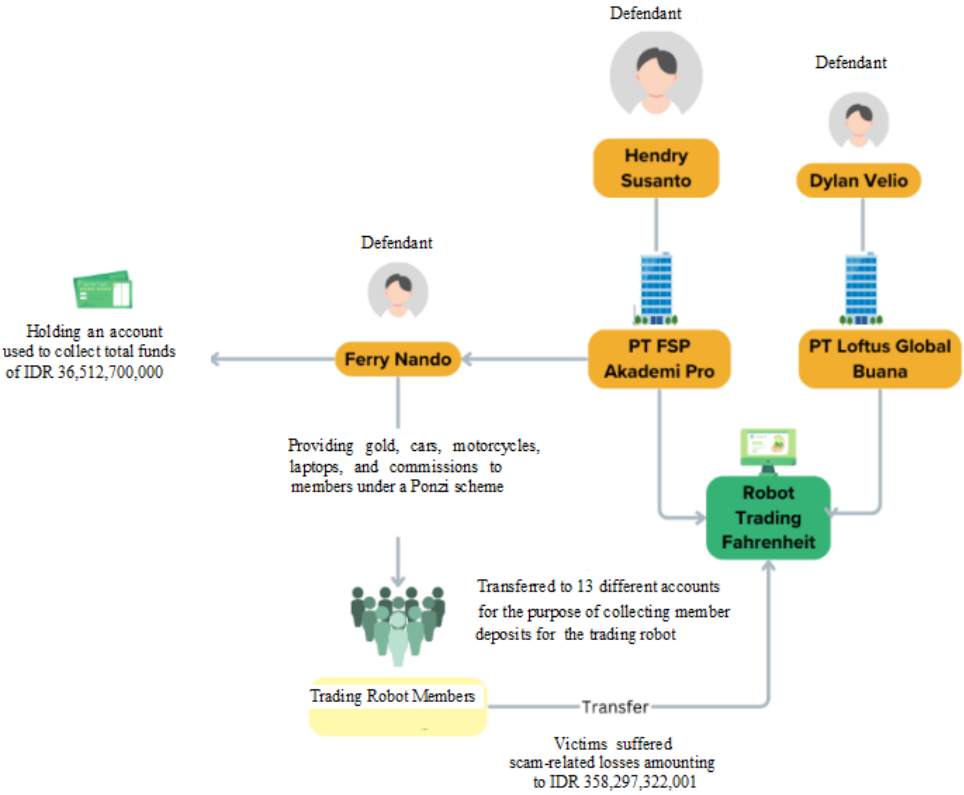

Figure 22 Overview of the Hendry Susanto Case

Case 8

Predicate Cybercrime: Phishing (Case in Australia)

A 24-year-old woman from Melbourne was sentenced for her significant role in a large international criminal syndicate that stole millions of dollars from innocent victims' pension savings and stock trading accounts through fraud and identity theft. The total amount stolen

through this fraud scheme was estimated to exceed AUD 3.3 million. Attempts were also made to steal an additional AUD 7.5 million from victims' pension savings and stock trading accounts. The group further laundered approximately AUD 2.5 million through the purchase and resale of luxury goods in Hong Kong. On 30 April 2019, investigators from the Australian Federal Police (AFP) and the Australian Securities and Investments Commission (ASIC) conducted a search of the woman's residence and examined her laptop and mobile phone, identifying details and images of hundreds of stolen identity documents.

The investigation, known as Operation Birks, revealed that the woman was operating as part of a large international criminal syndicate that used fraudulently obtained identities to carry out large-scale and sophisticated cybercrime. Stolen identity information was purchased from darknet markets, along with disposable SIM cards and fake email accounts, and used to carry out "identity takeovers" of unsuspecting victims. These false identities were created to closely mimic real individuals whose identities had been unknowingly compromised and were subsequently used to open bank accounts at various financial institutions across Australia. Investigators identified at least 60 bank accounts that were opened using these fake identities.

Once the fake identities and bank accounts had been established, the syndicate illegally accessed and stole funds from victims' pension savings and stock trading accounts. The offenders worked with others to create cloned websites that impersonated legitimate pension fund websites, using domain names that were nearly identical to the genuine sites. Online advertisements were used to promote these cloned websites so they would appear at the top of search engine results. The purpose was to capture members' usernames and passwords when they visited these cloned websites (phishing). The stolen member information was then used to obtain unauthorized access to victims' accounts. The syndicate withdrew pension fund savings from victims and deposited the funds into fraudulent bank accounts. The stolen funds were subsequently laundered by transferring them to overseas contacts, who used the money to purchase untraceable assets such as jewelry and luxury goods in Hong Kong. These goods were then resold, and the proceeds were sent back to the offenders in Australia via cryptocurrency.

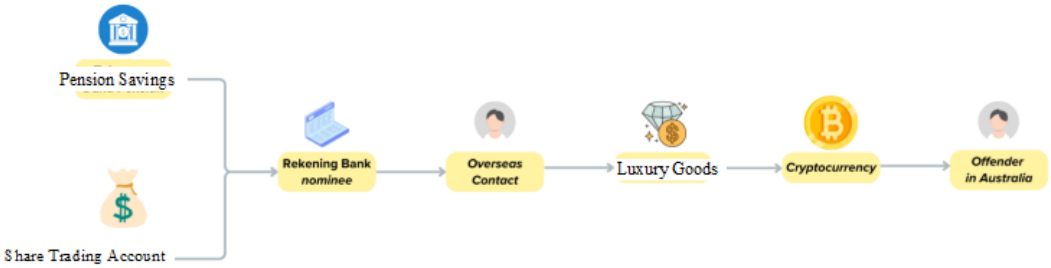

Figure 23 Overview of the Australia Phishing Case

CHAPTER V

CONCLUSIONS AND RISK MITIGATION STRATEGIES

5.1. Conclusions

Based on the results of the identification, analysis, and evaluation of Money Laundering (ML) and Terrorist Financing (TF) risks arising from Cybercrime, the following conclusions are drawn:

1. No evidence has been found indicating a shift in the risk level of Cybercrime/ITE as a predicate offense of money laundering following the 2021 National Risk Assessment (NRA). The risk of Cybercrime related to ML remains low, as reflected in the limited number of cybercrime cases that were charged with or proven to involve money laundering.
2. Based on the type of cybercrime, online fraud is assessed as posing a high risk for ML.
3. Based on the offender profile, entrepreneurs/self-employed individuals and private-sector employees are assessed as high-risk profiles for ML derived from cybercrime. Indonesian citizens are assessed as posing a high risk for ML derived from cybercrime. Proceeds of cybercrime also tend to be laundered by the cybercrime offenders themselves.
4. Based on geographical location, DKI Jakarta is assessed as having a high risk of ML derived from cybercrime.
5. Based on the reporting entity industry sector, the banking sector is assessed as high risk.
6. Based on money-laundering typologies, the typologies assessed as high risk are the use of virtual currencies and online gambling.
7. Based on transaction patterns, fund transfers and cash withdrawals/deposits are assessed as high risk.
8. Singapore, the United States, Hong Kong, the People's Republic of China, India, and Malaysia are identified by respondents as countries that potentially serve as source countries, destination countries, and transit countries for funds related to ML derived from cybercrime.

9. The risk level of terrorist financing (TF) could not be measured in this assessment due to data limitations. However, given the existence of cyber-fraud cases used as sources of terrorist financing funds abroad, this potential risk must be taken seriously.
10. The misuse of financial technology (e.g. crypto assets) and cyberspace for communication, propaganda, and recruitment has demonstrably occurred and requires heightened vigilance by law enforcement authorities. Emerging threats of emerging threats of ML and TF arising from cybercrime include:
    1) Misuse of Artificial Intelligence (AI)
    2) Misuse of e-wallets
    3) Use of coin-mixing services/coin mixers
    4) Distribution of links or files containing malware or designed to take over user data
    5) Use of private wallet addresses
    6) Exploitation of Web3 technology and crypto assets

5.2. RISK MITIGATION STRATEGIES

Based on the results of the identification of threats, vulnerabilities, impacts, and risks related to money laundering (ML) and terrorist financing (TF) arising from cybercrime, a risk evaluation has been conducted and risk mitigation strategies have been determined. These strategies may be implemented by all relevant stakeholders, including but not limited to the following:

a. Prevention Sector

No.	Prevention Strategies	Term	Responsible Party
1	Increase public awareness of cybercrime, for example the dangers of cybercrime and the impacts of buying and selling bank accounts	Medium	1. Ministry of Communication and Digital Affairs 2. National Cyber and Crypto Agency 3. Indonesian National Police
2	Develop suspicious transaction indicators (STR indicators) related to cybercrime	Medium	1. INTRAC 2. Indonesian National Police 3. Supervisory and Regulatory Authorities 4. Ministry of Communication and Digital Affairs 5. National Cyber and Crypto Agency

3	Enhance the use of technology in the prevention of cybercrime, particularly for cyber-attack prevention and detection of cybercrime-related transactions	Short	1. INTRAC 2. Indonesian National Police 3. Supervisory and Regulatory Authorities 4. Ministry of Communication and Digital Affairs 5. National Cyber and Crypto Agency
4	Strengthen the capacity of cybercrime supervisors and investigators in financial technology and crypto assets	Medium	1. INTRAC 2. Indonesian National Police 3. Supervisory and Regulatory Authorities 4. Ministry of Communication and Digital Affairs 5. National Cyber and Crypto Agency
5	Disseminate the results of the risk assessment	Short	1. INTRAC 2. Indonesian National Police 3. Supervisory and Regulatory Authorities 4. Ministry of Communication and Digital Affairs 5. National Cyber and Crypto Agency
6	Enhance the capacity of AML/CFT officers of reporting parties	Medium	1. INTRAC 2. Indonesian National Police 3. Supervisory and Regulatory Authorities 4. Ministry of Communication and Digital Affairs 5. National Cyber and Crypto Agency

b. Eradication Sector

No.	Eradication Strategy	Term	Responsible Party
1.	Strengthening regulations on Cyber Crime	Long	Government of the Republic of Indonesia
2.	Developing guidelines/Standard Operating Procedures (SOPs) for the seizure of Crypto Assets	Medium	1. Indonesian National Police 2. Attorney General's Office
3.	Establishing a single government wallet for the management of Crypto Asset evidence	Short	1. Indonesian National Police 2. Attorney General's Office

4.	Developing specific guidelines for the investigation of Cyber-based Money Laundering (ML) and Terrorist Financing (TF) offences	Medium	1. Indonesian National Police 2. Attorney General's Office

c. Cooperation Sector

No.	Eradication Strategy	Term	Responsible Party
1.	Strengthening cooperation in case handling, both domestically and internationally	Short	1. INTRAC 2. Indonesian National Police 3. Attorney General's Office 4. Mutual Legal Assistance Authority 5. Supervisory and Regulatory Authorities
2.	Enhancing cooperation in information exchange, both domestically and internationally	Short	1. INTRAC 2. Indonesian National Police 3. Attorney General's Office 4. Supervisory and Regulatory Authorities 5. Relevant Ministries/Agencies 6. Reporting-Entity Industry Associations 7. Reporting Parties 8. Marketplaces/E-commerce
3.	Enhancing cooperation in education and training, both domestically and internationally	Short	1. INTRAC 2. Indonesian National Police 3. Attorney General's Office 4. Supervisory and Regulatory Authorities 5. Relevant Ministries/Agencies 6. Reporting-Entity Industry Associations 7. Reporting Parties
4.	Enhancing the utilization of Public–Private Partnership (PPP) platforms for information exchange and the development of operational alerts (OAs) related to cybercrime	Short	1. INTRAC 2. Indonesian National Police 3. Attorney General's Office 4. Supervisory and Regulatory Authorities 5. Relevant Ministries/Agencies 6. Reporting Parties

Bibliography

Anjelina, C. D., & Afifah, M. N. (2024, June 29). *Kilas balik ransomware WannaCry: Pernah serang 150 negara termasuk Indonesia 7 tahun lalu*. Kompas. https://www.kompas.com/tren/read/2024/06/29/063000065/kilas-balik-ransomware-wannacry-pernah-serang-150-negara-termasuk-indonesia

Australian Strategic Policy Institute. (2021). *Counterterrorism yearbook 2021*. Australian Strategic Policy Institute.

Australian Strategic Policy Institute. (2022). *Counterterrorism yearbook 2022*. Australian Strategic Policy Institute.

Aziz, M. A. (2019). Pengembangan satuan unit cyber crime. *Jurnal Litbang Polri*, 22(1), 408–459.

Dimila, M. (2019, May 25). *Cerita Irdam tangani kasus cybercrime pertama di Indonesia. Dialeksis*: https://www.dialeksis.com/soki/cerita-irdam-tangani-kasus-cybercrime-pertama-di-indonesia/

Indonesia. (2008). *Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions*. State Gazette of the Republic of Indonesia Year 2008 Number 58, Supplement to the State Gazette Number 4843. Jakarta: State Secretariat.

Indonesia. (2016). *Law of the Republic of Indonesia Number 19 of 2016 on the Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*. State Gazette of the Republic of Indonesia Year 2016 Number 251, Supplement to the State Gazette Number 5952. Jakarta: State Secretariat.

Indonesia. (2024). *Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions*. State Gazette of the Republic of Indonesia Year 2024 Number 1, Supplement to the State Gazette Number 6905. Jakarta: State Secretariat.

Interpol. (2021). *ASEAN cyberthreat assessment 2021*. Retrieved from https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

Interpol. (2023). Interpol's 2023 global crime report. Retrieved from https://www.interpol.int/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports

Special Class I Batam Immigration Office. (2024, June 28). *Immigration Office detains 103 foreign nationals for immigration permit abuse and suspected cybercrime.* Retrieved November 28, 2024, from: https://kanimbatam.kemenkumham.go.id/berita/2024/06/imigrasi-amankan-103-wna-yang-menyalahgunakan-izin-tinggal-dan-diduga-melakukan-kejahatan-terkait-siber

Malik, N. (2018). *Terror in the dark: How terrorists use encryption, the darknet, and cryptocurrencies*. London, UK: The Henry Jackson Society.

Pusiknas Bareskrim Polri. (n.d.). *Kejahatan siber di Indonesia naik berkali-kali lipat*. Retrieved November 22, 2024, from https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

R, M. A. (2024, September 21). *Resmi, kini ada Direktorat Reserse Siber di Polda. Detik News*: https://news.detik.com/berita/d-7551640/resmi-kini-ada-direktorat-reserse-siber-di-8-polda

Sa'diyah, H. (2017, January 10). *Bahrun Naim sent funds via PayPal*. Retrieved November 28, 2024, from Republika: https://www.r epublika.co.id/berita/koran/hukum-koran/17/01/10/ojjy4633-bahrun-naim-kirim-dana-lewat-paypal

Tribratanews.polri.go.id. (2023, December 27). *Polri: Kasus Kejahatan Siber di 2023 Turun hingga 1.075 Perkara dari 2022*. Retrieved on November 28, 2024, from Tribratanews.polri.go.id: https://tribratanews.sulut.polri.go.id/polri-kasus-kejahatan-siber-di-2023-turun-hingga-1-075-perkara-dari-2022

U.S. Immigration and Customs Enforcement. (2020, August 13). *Global disruption of three terror finance cyber-enabled campaigns.* Retrieved November 22, 2024, from https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns

United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institute. (2024). *Beneath the surface: Terrorist and violent extremist use of the dark web and cybercrime as a service for cyber-attacks*. United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institute.

Wolf, A. (2024, April 19). A brief history of cybercrime. Arctic Wolf. Retrieved November 22, 2024, from https://arcticwolf.com/resources/blog/decade-of-cybercrime/

Wu, J., Lin, K., Lin, D., Zheng, Z., Huang, H., & Zheng, Z. (2023). Financial crimes in Web3-empowered metaverse: Taxonomy, countermeasures, and opportunities. IEEE Open Journal of the Computer Society, 4, 37–49. https://doi.org/10.1109/OJCS.2023.3245801.

APPENDICES

Table 4. Risk Level of Money Laundering from Cybercrime by Cybercrime Types

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Likelihood x Impact	Risk Scale	
1	Electronic system hacking	4.06	Low	4.46	Low	8.52	4.16	Low	4.83	Low	20.07	3.92	Low
2	Illegal interception	3.00	Low	3.27	Low	6.27	3.01	Low	3.00	Low	9.02	3.00	Low
3	Website defacement	3.36	Low	3.52	Low	6.89	3.32	Low	3.39	Low	11.25	3.19	Low
4	System interference	3.26	Low	3.00	Low	6.26	3.00	Low	3.53	Low	10.58	3.13	Low
5	Data manipulation	3.91	Low	4.01	Low	7.92	3.85	Low	4.72	Low	18.15	3.76	Low
6	Online pornography	4.14	Low	4.53	Low	8.67	4.23	Low	4.12	Low	17.46	3.70	Low
7	Online gambling	6.09	Medium	5.28	Medium	11.37	5.61	Medium	6.88	Medium	38.60	5.47	Medium
8	Online defamation	3.18	Low	3.18	Low	6.36	3.05	Low	3.00	Low	9.16	3.01	Low

9	Online fraud	9.00	High	9.00	High	18.00	9.00	High	9.00	High	81.00	9.00	High
10	Online threats and coercion	3.98	Low	3.35	Low	7.33	3.55	Low	3.72	Low	13.22	3.35	Low
11	Illegal access	4.32	Low	4.01	Low	8.32	4.06	Low	4.57	Low	18.54	3.79	Low
12	Data theft	4.13	Low	4.01	Low	8.14	3.96	Low	4.08	Low	16.17	3.60	Low

Table 5 Risk Level of Money Laundering from Cybercrime Based on Offender Profile

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Likelihood x Impact	Risk Scale	
1	Labourer, Domestic Worker and Security Staff	4.48	Low	4.71	Low	9.19	4.64	Low	4.69	Low	21.75	4.06	Low
2	Housewife	4.78	Low	6.2	Medium	10.97	5.56	Medium	4.24	Low	23.59	4.22	Low
3	Trader	5.1	Medium	7.06	High	12.16	6.18	Medium	5.73	Medium	35.39	5.2	Medium
4	Bank Employee	5.17	Medium	7.25	High	12.42	6.31	Medium	5.3	Medium	33.45	5.04	Medium
5	SOE/SROE Employee (incl. retirees)	4.45	Low	6.4	Medium	10.85	5.5	Medium	4.77	Low	26.2	4.43	Low

6	Money Changer Employee	4.65	Low	6.61	Medium	11.25	5.71	Medium	4.83	Low	27.55	4.55	Low
7	Private Employee	7.79	High	9.0	High	16.79	8.57	High	7.42	High	63.58	7.55	High
8	Legislative & Government Official	4.62	Low	6.87	Medium	11.49	5.83	Medium	5.83	Medium	33.96	5.08	Medium
9	Student	6.51	Medium	8.33	High	14.84	7.56	High	6.05	Medium	45.75	6.06	Medium
10	Teacher & Lecturer	4.11	Low	5.92	Medium	10.02	5.07	Medium	4.27	Low	21.68	4.06	Low
11	Craftsperson	3.0	Low	4.23	Low	7.23	3.62	Low	3.21	Low	11.65	3.22	Low
12	Foundation/Legal Entity Administrator	4.14	Low	5.48	Medium	9.62	4.86	Low	4.34	Low	21.12	4.01	Low
13	Political Party Official	4.68	Low	6.61	Medium	11.28	5.72	Medium	4.86	Low	27.8	4.57	Low
14	NGO/Non-corporated Organisation Staff	4.5	Low	5.77	Medium	10.28	5.2	Medium	4.51	Low	23.46	4.2	Low
15	Entrepreneur/ Business Owner	9.0	High	8.62	High	17.62	9.0	High	9.0	High	81.0	9.0	High
16	Farmer & Fisher	3.02	Low	3.0	Low	6.02	3.0	Low	3.0	Low	9.0	3.0	Low
17	Civil Servant (incl. retirees)	4.96	Low	5.99	Medium	10.94	5.55	Medium	5.26	Medium	29.2	4.68	Low
18	Professional & Consultant	5.04	Medium	6.4	Medium	11.44	5.8	Medium	5.86	Medium	34.01	5.08	Medium
19	Military/Police (incl. retirees)	4.4	Low	5.84	Medium	10.24	5.18	Medium	5.29	Medium	27.43	4.54	Low
20	Religious Leader	3.12	Low	4.63	Low	7.75	3.9	Low	3.54	Low	13.79	3.4	Low

Table 6. Risk Level of Money Laundering from Cybercrime Based on Region

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Likelihood x Impact	Risk Scale	
1	Aceh	3.49	Low	3.69	Low	7.18	3.57	Low	3.6	Low	12.86	3.32	Low
2	Bali	5.26	Medium	6.39	Medium	11.65	5.82	Medium	6.51	Medium	37.84	5.4	Medium
3	Banten	5.66	Medium	5.65	Medium	11.31	5.65	Medium	6.96	Medium	39.29	5.52	Medium
4	Bengkulu	3.37	Low	3.43	Low	6.8	3.38	Low	3.43	Low	11.61	3.22	Low
5	DI Yogyakarta	4.45	Low	5.65	Medium	10.11	5.04	Medium	4.46	Low	22.51	4.13	Low
6	DKI Jakarta	9.0	High	9.0	High	18.0	9.0	High	9.0	High	81.0	9.0	High
7	Gorontalo	3.43	Low	3.77	Low	7.2	3.58	Low	3.5	Low	12.54	3.3	Low
8	Jambi	3.4	Low	3.6	Low	7.0	3.48	Low	3.5	Low	12.19	3.27	Low
9	West Java	6.35	Medium	7.13	High	13.48	6.74	Medium	7.71	High	51.94	6.58	Medium
10	Central Java	5.05	Medium	6.45	Medium	11.5	5.74	Medium	5.58	Medium	32.05	4.92	Low
11	East Java	5.31	Medium	6.71	Medium	12.02	6.0	Medium	5.88	Medium	35.26	5.19	Medium
12	West Kalimantan	3.9	Low	4.41	Low	8.31	4.14	Low	3.7	Low	15.31	3.53	Low
13	South Kalimantan	3.49	Low	3.77	Low	7.26	3.61	Low	3.53	Low	12.77	3.31	Low

14	Central Kalimantan	3.43	Low	3.77	Low	7.2	3.58	Low	3.53	Low	12.66	3.31	Low
15	East Kalimantan	3.88	Low	4.01	Low	7.9	3.93	Low	4.52	Low	17.77	3.73	Low
16	North Kalimantan	3.3	Low	3.43	Low	6.74	3.35	Low	3.4	Low	11.39	3.2	Low
17	Bangka Belitung Islands	3.6	Low	3.69	Low	7.29	3.63	Low	4.37	Low	15.87	3.57	Low
18	Riau Islands	4.46	Low	4.41	Low	8.88	4.42	Low	6.64	Medium	29.39	4.7	Low
19	Lampung	4.26	Low	4.33	Low	8.59	4.28	Low	4.13	Low	17.67	3.72	Low
20	Maluku	3.2	Low	3.26	Low	6.47	3.22	Low	3.36	Low	10.82	3.15	Low
21	North Maluku	3.27	Low	3.18	Low	6.45	3.21	Low	3.33	Low	10.67	3.14	Low
22	West Nusa Tenggara	3.69	Low	3.6	Low	7.3	3.63	Low	3.4	Low	12.34	3.28	Low
23	East Nusa Tenggara	3.4	Low	3.43	Low	6.83	3.4	Low	3.36	Low	11.43	3.2	Low
24	Papua	3.27	Low	3.69	Low	6.96	3.46	Low	3.47	Low	12.0	3.25	Low
25	West Papua	3.14	Low	3.35	Low	6.49	3.23	Low	3.11	Low	10.04	3.09	Low
26	Central Papua	3.07	Low	3.26	Low	6.33	3.15	Low	3.15	Low	9.92	3.08	Low
27	Highland Papua	3.21	Low	3.18	Low	6.38	3.17	Low	3.11	Low	9.88	3.07	Low
28	South Papua	3.0	Low	3.09	Low	6.09	3.03	Low	3.0	Low	9.08	3.01	Low
29	Southwest Papua	3.03	Low	3.0	Low	6.03	3.0	Low	3.0	Low	9.0	3.0	Low
30	Riau	4.09	Low	4.41	Low	8.51	4.24	Low	3.86	Low	16.34	3.61	Low
31	West Sulawesi	3.54	Low	3.6	Low	7.15	3.56	Low	3.53	Low	12.57	3.3	Low
32	South Sulawesi	4.23	Low	4.41	Low	8.64	4.31	Low	4.67	Low	20.11	3.93	Low
33	Central Sulawesi	3.64	Low	4.01	Low	7.66	3.81	Low	3.6	Low	13.72	3.39	Low

34	Southeast Sulawesi	3.43	Low	3.69	Low	7.12	3.54	Low	3.43	Low	12.16	3.26	Low
35	North Sulawesi	3.58	Low	3.93	Low	7.52	3.74	Low	3.63	Low	13.59	3.38	Low
36	West Sumatra	3.73	Low	4.01	Low	7.74	3.86	Low	4.49	Low	17.32	3.69	Low
37	South Sumatra	4.93	Low	5.72	Medium	10.65	5.31	Medium	5.3	Medium	28.17	4.6	Low
38	North Sumatra	4.99	Low	5.45	Medium	10.44	5.21	Medium	5.27	Medium	27.47	4.54	Low

Table 7 Risk Level of Money Laundering from Cybercrime by Offender Nationality

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Risk		Risk Level
						Total	Likelihood Scale			Impact Level	Risk Scale	
1	Indonesian Citizen (WNI)	9.00	High	9.00	High	18.00	9.00	High	9.00	High	81.00	High
2	Foreign National (WNA)	3.00	Low	3.00	Low	6.00	3.00	Low	3.00	Low	9.00	Low

Table 8 Risk Level of Money Laundering Based on Whether the Cybercrime Offender Is Also a Money Laundering Offender

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Likelihood x Impact	Risk Scale	
1	Cybercrime offender who is also a money laundering offender	9.00	High	9.00	High	18.00	9.00	High	9.00	High	81.00	9.00	High
2	Cybercrime offender who is not a money laundering offender	3.00	Low	3.00	Low	6.00	3.00	Low	3.00	Low	9.00	3.00	Low

Table 9. Risk Level of Money Laundering from Cybercrime Based on Reporting Party's Industrial Sector

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Total	Likelihood Scale	Likelihood Level	Impact Scale	Impact Level	Likelihood x Impact	Risk Scale	Risk Level
1	Bank	9.0	High	9.0	High	18.0	9.0	High	9.0	High	81.0	9.0	High
2	Finance Companies	4.06	Low	5.51	Medium	9.57	4.75	Low	4.04	Low	19.23	3.85	Low
3	Insurance Companies and Insurance Brokers	3.72	Low	4.73	Low	8.45	4.19	Low	3.6	Low	15.08	3.51	Low
4	Pension Funds / Financial Institutions	3.42	Low	4.21	Low	7.63	3.78	Low	3.47	Low	13.11	3.34	Low
5	Securities Companies	4.27	Low	5.72	Medium	9.98	4.96	Low	4.38	Low	21.72	4.06	Low
6	Investment Managers	4.21	Low	5.58	Medium	9.8	4.87	Low	4.29	Low	20.91	3.99	Low
7	Custodians	3.51	Low	3.98	Low	7.49	3.71	Low	3.69	Low	13.68	3.39	Low
8	Trustees	3.42	Low	3.66	Low	7.08	3.5	Low	3.24	Low	11.35	3.2	Low
9	Money Services Providers	3.3	Low	3.42	Low	6.72	3.32	Low	3.24	Low	10.76	3.15	Low
10	Foreign Exchange Traders	5.69	Medium	6.69	Medium	12.38	6.17	Medium	4.66	Low	28.76	4.65	Low

11	Payment System Operators Using Cards	4.34	Low	5.38	Medium	9.72	4.83	Low	4.07	Low	19.67	3.89	Low
12	E-Money and E-Wallet Operators	6.01	Medium	7.06	High	13.07	6.52	Medium	4.69	Low	30.54	4.79	Low
13	Savings and Loan Cooperatives	3.51	Low	4.66	Low	8.17	4.05	Low	3.5	Low	14.19	3.43	Low
14	Pawnshops	3.26	Low	4.05	Low	7.32	3.62	Low	3.1	Low	11.24	3.19	Low
15	Commodity Futures Trading Companies	4.77	Low	5.02	Medium	9.79	4.87	Low	6.02	Medium	29.28	4.69	Low
16	Physical Crypto Asset Traders	5.97	Medium	8.1	High	14.06	7.02	High	5.41	Medium	37.95	5.41	Medium
17	Money Transfer Service Providers	5.34	Medium	6.37	Medium	11.71	5.83	Medium	4.76	Low	27.77	4.56	Low
18	Property Companies/Agents	4.53	Low	5.58	Medium	10.11	5.03	Medium	4.07	Low	20.47	3.96	Low
19	Motor Vehicle Dealers	4.57	Low	5.58	Medium	10.16	5.05	Medium	4.04	Low	20.42	3.95	Low
20	Primary Gold and Precious Metals Dealers	4.67	Low	6.31	Medium	10.98	5.47	Medium	4.58	Low	25.06	4.34	Low
21	Art and Antique Dealers	3.91	Low	4.73	Low	8.64	4.29	Low	3.66	Low	15.69	3.56	Low
22	Auction Houses	3.3	Low	4.13	Low	7.43	3.68	Low	3.44	Low	12.64	3.3	Low

23	Venture Capital Companies	3.39	Low	3.9	Low	7.29	3.61	Low	3.53	Low	12.74	3.31	Low
24	Infrastructure Financing Companies	3.17	Low	3.74	Low	6.91	3.41	Low	3.34	Low	11.4	3.2	Low
25	Microfinance Institutions	3.33	Low	3.98	Low	7.3	3.61	Low	3.21	Low	11.59	3.22	Low
26	Export Financing Institutions	3.2	Low	4.21	Low	7.41	3.67	Low	3.47	Low	12.72	3.31	Low
27	Technology‑Based Lending Platforms	4.14	Low	5.85	Medium	9.99	4.97	Low	4.27	Low	21.19	4.02	Low
28	Equity Crowdfunding Platforms	4.19	Low	5.02	Medium	9.22	4.58	Low	4.18	Low	19.15	3.85	Low
29	IT‑Based Financial Transaction Service Providers	4.19	Low	5.85	Medium	10.04	4.99	Low	4.21	Low	21.03	4.0	Low
30	Advocates (Lawyers)	3.17	Low	3.58	Low	6.75	3.33	Low	3.21	Low	10.69	3.14	Low
31	Notaries	3.64	Low	4.13	Low	7.77	3.85	Low	3.53	Low	13.61	3.38	Low
32	Land Deed Officials	3.51	Low	4.05	Low	7.57	3.75	Low	3.44	Low	12.88	3.32	Low
33	Accountants	3.2	Low	3.25	Low	6.45	3.18	Low	3.07	Low	9.78	3.06	Low
34	Public Accountants	3.0	Low	3.08	Low	6.08	3.0	Low	3.0	Low	9.0	3.0	Low
35	Financial Planners	3.17	Low	3.0	Low	6.17	3.04	Low	3.21	Low	9.75	3.06	Low

Table 10 Risk Level of Money Laundering from Cybercrime Based on Money Laundering Typology

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Likelihood × Impact	Risk Scale	
1	Use of false identities	7.19	High	8.31	High	16	7.63	High	5.83	Medium	44.51	6.57	Medium
2	Property/real estate, including the role of property agents	4.26	Low	5.61	Medium	10	4.56	Low	4.22	Low	19.23	4.0	Low
3	Use of nominees (borrowed names, trusts, family members, or third parties)	7.59	High	7.49	High	15	7.4	High	5.3	Medium	39.2	6.03	Medium
4	Smurfing	6.56	Medium	8.31	High	15	7.29	High	5.74	Medium	41.86	6.3	Medium

5	Structuring	6.9	Medium	7.9	High	15	7.25	High	5.57	Medium	40.38	6.15	Medium
6	Use of professional services	3.11	Low	3.91	Low	7	3.0	Low	3.12	Low	9.35	3.0	Low
7	Use of new payment methods/systems	6.53	Medium	6.63	Medium	13	6.35	Medium	4.63	Low	29.38	5.03	Medium
8	Use of legal persons	4.32	Low	4.9	Low	9	4.2	Low	3.58	Low	15.02	3.58	Low
9	Use of non-bank sectors	5.07	Medium	8.21	High	13	6.42	Medium	5.06	Medium	32.48	5.35	Medium
10	Use of non-financial sectors	3.69	Low	4.66	Low	8	3.73	Low	3.63	Low	13.53	3.42	Low
11	Foreign currency exchange	5.68	Medium	6.29	Medium	12	5.71	Medium	4.32	Low	24.67	4.56	Medium
12	Mingling (mixing illicit funds with legal business funds)	6.42	Medium	7.17	High	14	6.59	Medium	5.16	Medium	33.96	5.5	Medium
13	Use of credit cards, cheques, cash transfer letters, and	3.44	Low	4.41	Low	8	3.46	Low	3.58	Low	12.35	3.3	Low

	money laundering techniques												
14	Trade-based money laundering and transfer pricing	3.87	Low	5.38	Medium	9	4.21	Low	3.9	Low	16.45	3.72	Low
15	Trade in precious metals	3.87	Low	5.84	Medium	10	4.47	Low	6.66	Medium	29.75	5.07	Medium
16	Use of illegal banks/unofficial value transfer services	7.33	High	8.11	High	15	7.6	High	9.0	High	68.4	9.0	High
17	Use of foreign banks/international banks	4.46	Low	5.49	Medium	10	4.6	Low	4.58	Low	21.07	4.19	Low
18	Use of offshore banks, shell companies, and international financing centers	4.75	Low	6.41	Medium	11	5.26	Medium	4.58	Low	24.06	4.49	Low
19	Trade in securities/commodities	3.72	Low	3.53	Low	7	3.12	Low	3.12	Low	9.73	3.04	Low

20	Trade in art, antiques, and collectibles	6.53	Medium	5.61	Medium	12	5.8	Medium	4.38	Low	25.36	4.63	Low
21	Online gambling activities	9.0	High	9.0	High	18	9.0	High	6.0	Medium	54.03	7.54	High
22	International transfers/use of foreign banks	5.79	Medium	5.02	Medium	11	5.07	Medium	8.29	High	41.99	6.32	Medium
23	Use of internet (access to personal data, online banking, etc.)	5.83	Medium	7.59	High	13	6.49	Medium	5.39	Medium	34.99	5.6	Medium
24	Commodity exchange (barter, including reinvestment in prohibited medicines)	3.0	Low	4.04	Low	7	3.01	Low	3.46	Low	10.42	3.11	Low
25	Investment in capital markets, precious metals, and mining	3.7	Low	3.66	Low	7	3.18	Low	3.52	Low	11.19	3.19	Low

26	Human smuggling	6.04	Medium	3.0	Low	9	4.1	Low	3.0	Low	12.31	3.3	Low

Table 11 Risk Level of Money Laundering from Cybercrime Based on Transaction Patterns

No.	Point of Concern	Threat Scale	Threat Level	Vulnerability Scale	Vulnerability Level	Likelihood		Likelihood Level	Impact Scale	Impact Level	Risk		Risk Level
						Total	Likelihood Scale				Risk (Likelihood x Impact)	Risk Scale	
1	Cash deposit/withdrawal	7.65	High	7.66	High	15	7.86	High	8.57	High	67.35	7.84	High
2	Cheque	5.6	Medium	3.91	Low	10	4.82	Low	3.76	Low	18.1	3.66	Low
3	Transfer	9.0	High	8.49	High	17	9.0	High	9.0	High	81.0	9.0	High
4	Internet banking / mobile banking	6.59	Medium	7.82	High	14	7.38	High	5.94	Medium	43.85	5.84	Medium
5	Virtual account	6.64	Medium	7.11	High	14	7.04	High	5.52	Medium	38.83	5.42	Medium

6	Foreign exchange trading	5.2	Medium	6.28	Medium	11	5.85	Medium	4.67	Low	27.34	4.44	Low
7	Purchase of property assets	5.48	Medium	6.28	Medium	12	6.0	Medium	4.52	Low	27.13	4.42	Low
8	Purchase of vehicles	4.77	Low	6.28	Medium	11	5.62	Medium	4.29	Low	24.12	4.17	Low
9	Purchase of other goods (besides assets)	5.08	Medium	5.59	Medium	11	5.42	Medium	3.93	Low	21.3	3.93	Low
10	Use of technology services	5.47	Medium	6.37	Medium	12	6.04	Medium	4.86	Low	29.33	4.61	Low
11	Cross-border cash transportation	3.78	Low	4.68	Low	8	4.27	Low	3.8	Low	16.21	3.5	Low
12	Antique goods purchase	3.49	Low	4.96	Low	8	4.26	Low	3.67	Low	15.64	3.45	Low
13	Auction purchase	3.44	Low	4.3	Low	8	3.89	Low	3.41	Low	13.27	3.25	Low
14	Purchase of gold/precious metals	4.26	Low	6.03	Medium	10	5.22	Medium	4.21	Low	21.99	3.99	Low
15	Purchase of insurance policy	3.0	Low	3.91	Low	7	3.45	Low	3.0	Low	10.36	3.0	Low
16	Purchase of capital market products	4.49	Low	5.59	Medium	10	5.12	Medium	4.13	Low	21.13	3.91	Low

17	Purchase of crypto assets	7.71	High	9.0	High	17	8.59	High	5.84	Medium	50.21	6.38	Medium
18	Use of electronic payment instruments / e-wallets	5.7	Medium	7.58	High	13	6.79	Medium	5.11	Medium	34.69	5.07	Medium
19	Cross-border instruments (e.g. traveller's cheques, bills of exchange, certificates of deposit)	3.05	Low	3.0	Low	6	3.0	Low	4.71	Low	14.13	3.32	Low
20	Inter-party transactions	4.63	Low	6.62	Medium	11	5.73	Medium	4.52	Low	25.89	4.32	Low

Indonesian Financial Transaction Reports and Analysis Center (INTRAC)

Jl. Ir. H Juanda No. 35 Jakarta 10120 Indonesia
Phone: (+6221) 3850455, 3853922
Fax: (+6221) 3856809 - 3856826
Website: http://www.ppatk.go.id